Release Notes:
Version K.14.84 Software
for the HP Series 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl Switches

These release notes include information on the following:

- This software is supported on the following switches

  HP ProCurve Switch 3500-24 (J9470A)
  HP ProCurve Switch 3500-24-PoE (J9471A)
  HP ProCurve Switch 3500-48 (J9472A)
  HP ProCurve Switch 3500-48-PoE (J9473A)
  HP ProCurve Switch 3500yl-24G-PWR Intelligent Edge (J8692A)
  HP ProCurve Switch 3500yl-48G-PWR Intelligent Edge (J8693A)
  HP ProCurve Switch 5406zl Intelligent Edge (J8697A)
  HP ProCurve Switch 5412zl Intelligent Edge (J8698A)
  HP ProCurve Switch 5406zl-48G Intelligent Edge (J8699A)
  HP ProCurve Switch 5412zl-96G Intelligent Edge (J8700A)
  HP ProCurve 5406zl-48G-PoE+ Switch (J9447A)
  HP ProCurve 5412zl-96G-PoE+ Switch (J9448A)
  HP ProCurve Switch 6200yl-24G-mGBIC (J8992A)
  HP ProCurve Switch 6600-24G (J9263A)
  HP ProCurve Switch 6600-24G-4XG (J9264A)
  HP ProCurve Switch 6600-24XG (J9265A)
  HP ProCurve Switch 6600-48G (J9451A)
  HP ProCurve Switch 6600-48G-4XG (J9452A)
  HP ProCurve Switch 8206zl (J9475A)
  HP ProCurve Switch 8212zl (J8715A/B)

  Downloading switch software and documentation from the Web (page 2)

- Best practices for major software updates, including contingency procedures for rolling back to previous software versions and configurations. **Please read before updating one major software version to the next.** (page 5).
- Notes for ROM updates (page 14)
- Clarifications for certain software features (page 17)
- A listing of software enhancements (page 24)
- A listing of software fixes (page 157)
- Support Notes and Known Issues (page 15)—includes "Security notes about SNMP access to the hpSwitchAuth MIB objects" and other topics.

Manual Part Number

5992-5498
June 2011

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation.
Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

Software Credits

SSH on HP Switches is based on the OpenSSH software toolkit. This product includes software developed by the OpenSSH Project for use in the OpenSSH Toolkit. For more information on OpenSSH, visit www.openssh.com.

SSL on HP Switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit www.openssl.org.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com) Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

For HP networking warranty information, visit www.hp.com/networking/support

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.hp.com/networking/support

Contents

Software Management

Support Notes

Clarifications

Known Issues

Enhancements

Software Fixes

Software Management

Premium License Switch Software Features

The HP ProCurve Switch 8200zl, 5400zl, and 3500 series use the same software image base and ship with Intelligent Edge and IP-based routing feature sets standard. For these switches, an optional Premium License is available to enable Advanced Routing features. NOTE: Legacy HP ProCurve Switch 8212zl (J8715A) products were shipped with Advanced Routing features standard—no Premium License upgrade is required for these switches. For a detailed listing of these functionalities, please see the data sheets for the HP ProCurve Switch 8200zl, 5400zl, and 3500 series on our website at: www.procurve.com.

Additional features might be required for deployments in the aggregation/distribution layer or if full routing is required in the wiring closet. To meet these requirements, HP provides the Premium License that contains the following features:

- OSPF
- PIM Sparse
- PIM Dense
- VRRP
- Q-in-Q (IEEE 802.1ad)

While all 8200zl, 5400zl, and 3500 series switches include Routing Information Protocol (RIP) that could be used to route IP traffic, OSPF is a better choice in all but the smallest environments. RIP is primarily used to provide a way to get network traffic from one VLAN to another in small environments.

To enable Advanced Routing feature set, please order the Premium License specific to the switch series:

- 8200zl series: J9474A—HP ProCurve Switch 8200zl Premium License
- 5400zl series: J8994A—HP ProCurve Switch 5400zl Premium License
- 3500 series: J8993A—HP ProCurve Switch 3500 Premium License

Each Premium License product provides license-to-use for a single 8200zl/5400zl/3500 series switch. Each license can be added to the switch manually through the MyProCurve Portal website using the registration ID included with the Premium License, along with some information obtained from the switch. The portal will then provide a license key that is entered into the switch and will enable the features.

HP ProCurve Manager (PCM) or ProCurve Manager Plus can be used to simplify the process of adding licenses. Just provide the registration ID from the Premium License and tell PCM onto which switch to install the license. PCM will communicate with the MyProCurve Portal directly and add the license to the switch without user intervention.

A previously installed license can be removed from an 8200zl, 5400zl, or 3500 series switch and transferred to another switch within the same product series.

All software features are automatically enabled on the ProCurve 6200yl switches without the need for a Premium License.

To view or download a listing of Intelligent Edge and Premium License features, refer to the Software Features Index available for download on the product documentation page for your switch model.

Note Switch software Version K.11.33 software or newer is required for proper functioning of Intelligent Edge features on ProCurve Switch 3500yl series, and ProCurve Switch 5400zl series.

Software Updates

Check the HP networking web site frequently for software updates for the various HP switches you may have in your network.

Download Switch Documentation and Software from the Web

You can download software updates and the corresponding product documentation from the HP networking web site. Check the Web site frequently for the latest software version available for your switch.

Viewing or Downloading the Software Manual Set

To view or download documentation, go to: **www.hp.com/networking/support**

Downloading Software Updates for Your Switch

HP periodically provides switch software updates through the HP networking web site (**www.hp.com/networking/support**). After you acquire the new software file, you can use one of the following methods for downloading it to the switch:

- For a TFTP transfer from a server, do either of the following:
  - Select **Download OS** in the Main Menu of the switch's menu interface and use the (default) **TFTP** option.
  - Use the **copy tftp** command in the switch's CLI (see below).
- For an Xmodem transfer from a PC or Unix workstation, do either of the following:
  - Select **Download OS** in the Main Menu of the switch's menu interface and select the **XMODEM** option.
  - Use the **copy xmodem** command in the switch's CLI (page 3).
- Use the USB port to download a software file from a USB flash drive (page 4).
- Use the download utility in ProCurve Manager Plus management software.

Note Downloading new software does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, to archive or to be used in another switch of the same model.

TFTP Download from a Server

Syntax: copy tftp flash <***ip-address***> <***remote-os-file***> [< primary | secondary >]

Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

For example, to download a software file named K_11_1x.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
ProCurve # copy tftp flash 10.28.227.103 K_11_1x.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message

```
Validating and Writing System Software to FLASH...
```

3. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:
   a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
   b. Reboot the switch from the flash area that holds the new software (primary or secondary), using the following command:

      Syntax: boot system flash [< primary | secondary >]

   After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.
4. Verify the software version by displaying the system information for the switch (for example, through the **show system-information** command), and viewing the `Software revision` field.

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (Refer to the *Installation and Getting Started Guide* you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with Windows NT, you would use the Send File option in the Transfer drop-down menu.)

Using Xmodem and a terminal emulator, you can download a switch software file to either primary or secondary flash using the CLI.

Syntax: copy xmodem flash [< primary | secondary >]

1. To reduce the download time, you may want to increase the baud rate in your terminal emulator and in the switch to a value such as 115200 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 115200, execute this command:

   ```
   ProCurve(config)# console baud-rate 115200
   ```

   (If you use this option, be sure to set your terminal emulator to the same baud rate.)

   Changing the console baud-rate requires saving to the Startup Config with the "write memory" command. Alternatively, you can logout of the switch and change your terminal emulator speed and allow the switch to AutoDetect your new higher baud rate (i.e. 115200 bps)
2. Execute the following command in the CLI:

   ```
   ProCurve # copy xmodem flash primary
   The primary OS image will be deleted. continue [y/n]? Y
   Press 'Enter' and start XMODEM on your host...
   ```

3. Execute the terminal emulator commands to begin the Xmodem transfer. For example, using HyperTerminal:
   a. Click on **Transfer**, then **Send File**.
   b. Type the file path and name in the **Filename** field.
   c. In the Protocol field, select **Xmodem**.
   d. Click on the **Send** button.

   The download can take several minutes, depending on the baud rate used in the transfer.

4. If you increased the baud rate on the switch (step 1), use the same command to return it to its previous setting. (ProCurve recommends a baud rate of 9600 bits per second for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.)
5. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
6. Reboot the switch from the flash area that holds the new software (primary or secondary).

   After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

Using USB to Download Switch Software

To use the USB port on the switch to download a software version from a USB flash drive:

- The software version must be stored on the USB flash drive, and you must know the file name (such as K_12_10.swi).
- The USB flash drive must be properly installed in the USB port on the switch.

Note Some USB flash drives may not be supported on your switch. For information on USB device compatibility, refer to the HP networking support website:

www.hp.com/networking/support.

Syntax: copy usb flash <***filename***> [< primary | secondary >]

For example, to download a software file named K_12_10.swi from a USB flash drive:

1. Execute the copy command as shown below:

```
ProCurve # copy usb flash K_12_10.swi secondary
The secondary OS image will be deleted. continue [y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message

```
Validating and Writing System Software to FLASH...
```

3. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:
   a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
   b. Reboot the switch from the flash area that holds the new software (primary or secondary), using the following command:

      Syntax: boot system flash [< primary | secondary >]

   After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.
4. Verify the software version by displaying the system information for the switch (for example, through the **show system-information** command), and viewing the `Software revision` field.

Saving Configurations While Using the CLI

The switch operates with two configuration files:

- **Running-Config File:** Exists in volatile memory and controls switch operation. Rebooting the switch erases the current running-config file and replaces it with an exact copy of the current startup-config file. To save a configuration change, you must save the running configuration to the startup-config file.
- **Startup-Config File:** Exists in flash (non-volatile) memory and preserves the most recently-saved configuration as the "permanent" configuration. When the switch reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory.

When you use the CLI to make a configuration change, the switch places the change in the running-config file. If you want to preserve the change across reboots, you must save the change to the startup-config file. Otherwise, the next time the switch reboots, the change will be lost. There are two ways to save configuration changes while using the CLI:

- Execute **write memory** from the Manager, Global, or Context configuration level.
- When exiting from the CLI to the Main Menu, press **[Y]** (for `Yes`) when you see the "save configuration" prompt:

```
Do you want to save current configuration [y/n]?
```

Best Practices for Major Software Updates

Major software updates contain new features and enhancements, and are designated by an increment to the major release version number. That is, K.12.xx represents a major update to software version(s) K.11.xx, and K.13.xx represents a major update to K.12.xx, and so forth. To mitigate against potential migration issues when performing such an update, this section documents best practices for updating the switch, including contingency procedures for rolling back to previous software versions and saved configurations.

Caution Before you update the switch software to a major new version, ProCurve strongly recommends that you save off a copy of your config file to an external location. ProCurve advises against rolling back (going from a newer software version to an older software version) without copying on a backup config file to the device.

Updating the Switch: Overview

To perform a major update to your switch software, follow the steps below (see page 6 for details):

1. Download the image to your TFTP server.
2. Save your current configuration (Config1) to a backup configuration file (Config2).
3. Save your current configuration to an external tftp server.
4. Backup your current running image (Primary) to the secondary image.
5. Set your secondary image to boot with Config2.
6. Download the new image to the switch's primary image.
7. Verify that your images and configuration are set correctly.
8. Reload the switch.

After following these steps, you should end up with the following results:

- Primary image will hold the new software image you want to install (for example, K.13.06)
- Secondary image will hold the image you are currently running (for example, K.12.57)
- Primary image will boot with config1 (config file corresponding to new software version—in this example, K.13.06)
- Secondary image will boot with config2* (config file corresponding to previous software version—in this example, K.12.57)

* The current config file must be copied to config2, or you will be unable to revert if the need arises.

Note: You might opt to use a different methodology in which the new software will be installed as the secondary and not the primary image, in which case you would use the commands **boot system flash secondary**, and/or **boot set-default flash secondary** to change the location of the default boot. However, since you will still need to take precautions to allow you to revert to your previous configuration, ProCurve strongly recommends you follow the methods that are proposed in our update process. This will ensure that you can use our proposed roll back procedures should the need arise.

Updating the Switch: Detailed Steps

The following detailed steps shows how to update the switch software from an existing version to a major new release (in the example provided here, from version K.12.57 to version K.13.06).

1. Download the latest release software image to your TFTP server from the HP website.: http://www.hp.com/networking/support
2. Save your current configuration (Config1) to backup configuration file (Config2).
   a. Before copying the config, verify the current state of your system using the **show version**, **show flash**, and **show config files** commands. For example:

```
Switch1# show version
Image stamp:    /sw/code/build/btm(t2g)
                Dec  7 2007 14:54:57
                K.12.57
                2415
Boot Image:     Primary

Switch1# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 6782942   12/07/07 K.12.57
Secondary Image : 6765066   08/24/07 K.12.43
Boot Rom Version: K.12.12
Default Boot    : Primary

Switch1# show config files

Configuration files:

 id | act pri sec | name
 ---+-------------+-------------------------------------------
  1 |  *   *   *  | config1
  2 |             |
  3 |             |
```

b. Create a backup configuration file and verify the change.

```
Switch1# copy config config1 config config2
Switch1# show config files

Configuration files:

 id | act pri sec | name
 ---+-------------+--------------------------------------------
  1 |  *   *   *  | config1
  2 |             | config2
  3 |             |
```

3. Save the current config to a tftp server using the **copy tftp** command. For example:

```
Switch1# copy startup-config tftp 10.1.1.60 Switch1_config_K_12_57.cfg
```

Note This step is necessary because ProCurve does not support roll back (going from a newer software version to an older software version) without the ability to copy a backup config file onto the device.

4. Backup your current running image (primary) to the secondary image.

```
Switch1# copy flash flash secondary

Switch1# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 6782942   12/07/07 K.12.57
Secondary Image : 6782942   12/07/07 K.12.57
Boot Rom Version: K.12.12
Default Boot    : Primary
```

5. Set your secondary image to boot with Config2.

```
Switch1# startup-default secondary config config2

Switch1# show config files

Configuration files:

 id | act pri sec | name
 ---+-------------+-------------------------------------------------
  1 |  *   *      | config1
  2 |          *  | config2
  3 |             |
```

Note This step will enable you to revert from K_13_05 to your previous image with your previous configuration just by invoking the command **boot system flash secondary**.

6. Download the new primary image.

```
Switch1# copy tftp flash 192.168.1.60 K_13_06.swi primary
The Primary OS Image will be deleted, continue [y/n]?
```

At the prompt, answer **y**, for yes, and the new image will be downloaded and written to the File system. Once tftp download has been completed you will see the following message:

```
Validating and Writing System Software to the Filesystem ...
```

7. Verify that your images and configuration are set correctly. For example, if you updated from K.12.57 to K.13.06, you should see the following outputs from the switch show commands:

```
Switch1# show version
Image stamp:    /sw/code/build/btm(t2g)
                Mar 14 2008 09:59:53
                K.12.57
                2415
Boot Image:     Primary


Switch1# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 7350018   03/14/08 K.13.06
Secondary Image : 6782942   12/07/07 K.12.57
Boot Rom Version: K.12.12
Default Boot    : Primary


Switch1# show config files

Configuration files:

 id | act pri sec | name
 ---+-------------+-------------------------------------------------
  1 |  *   *      | config1
  2 |          *  | config2
  3 |             |
```

8. Reload the new switch image.

```
Switch1# reload
System will be rebooted from primary image. Do you want to continue [y/n]?  y
```

At the prompt, answer **y**, for yes, and the switch will boot with the new image.

Note: As an additional step, ProCurve advises saving the startup-config to a tftp server using the **copy tftp** command. For example:

```
Switch1# copy startup-config tftp 10.1.1.60 Switch1_config_K_13_06.cfg
```

Rolling Back Switch Software

If you have followed the update procedures documented in the previous section, you should be able to revert to your previous configuration and software version using the steps below.

To roll back your switch from K.13.06 to K.12.57, for example, follow the steps below:

1. Verify that your images and configuration are set correctly using the **show version**, **show flash**, and **show config files** commands.

```
Switch1# show version
Image stamp:    /sw/code/build/btm(t2g)
                Mar 14 2008 09:59:53
                K.13.06
                211
Boot Image:     Primary


Switch1# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 7350018   03/14/08 K.13.06
Secondary Image : 6782942   12/07/07 K.12.57
Boot Rom Version: K.12.12
Default Boot    : Primary


Switch1# show config files

Configuration files:

 id | act pri sec | name
 ---+-------------+-------------------------------------------------
  1 |  *   *      | config1
  2 |          *  | config2
  3 |             |
```

2. Boot the switch using the secondary image (with config2).

```
Switch1# boot system flash secondary
System will be rebooted from secondary image. Do you want to continue [y/n]?  y
```

Answer **y**, for yes, and the switch will boot from the secondary image (K.12.57, in this example) with the corresponding configuration for that software version (Config2).

Viewing or Transferring Alternate Configuration Files

Viewing or copying an alternate configuration saved to the switch will always be accomplished through the software currently running on the switch. This may result in a misleading portrayal of the configuration. For example, if a configuration is created on K.12.57 and saved as config2, and if it is then viewed or transferred while the switch is running K.13.06, it will appear as though K.13.06 has converted the configuration. However, the alternate configuration file, config2, will still be intact on the switch and load properly when the switch is booted into the same software version from which the configuration file originated.

When an enhancement introduces a feature that did not previously exist in the switch, it may present several challenges to the user.

Backwards compatibility of the configuration created with a version of software that supports a new feature or parameter is not guaranteed. Software versions that did not recognize or support a particular command or parameter will not be able to interpret that line in the configuration. For this reason, it is strongly recommended that network administrators always save their configuration *while still running the switch with the original software version*, and with a notation indicating the software version on which the configuration was saved. For example, a user might save a configuration for a switch running K.12.57 to a TFTP server with an IP address of 10.10.10.15 as follows:

```
ProCurve5406zl-onK1257# copy running-config tftp 10.10.10.15 5406onK1257
```

If, for example, the user deems it necessary to revert to the use of K.12.57, she can boot into it and then restore the saved config from the TFTP server.

Viewing or copying an alternate configuration that is saved to the switch flash can be accomplished only with the software that is currently running on the switch.

Here, for example, a configuration is created on K.12.57 and then saved to flash:

```
ProCurve5406zl-onK1257# copy config config2 config K1257config <cr>
```

And later, the configuration that was created on K.12.57 is viewed while the switch is running K.13.06:

```
ProCurve5406zl-onK1306# show config K1257config <cr>
```

The command output will show how the K.12.57 config would be interpreted, *if it were to be used by the K.13.06 software*. Copying the K1257config to a TFTP server would similarly trigger an interpretation by the software performing the file transfer. Note, however, that this does not actually *change* the configuration. If the version is rolled back from K.13.06 to K.12.57 with a command like the following (given that K.12.57 is stored in secondary flash), the K.12.xx formatted config is still intact and valid.

```
ProCurve5406zl# boot system flash secondary config K1257config
```

This "interpretation" during a TFTP or **show** command execution is inherent in the architecture of the switch. When switch features change significantly (e.g. the move from IPv4 support to IPv6 support), there may be configuration parameters from the previous config that cannot be translated by the switch for viewing while it is running the new software. This necessitates storing configurations for each version of software to an external location, if the user would like to view the stored config prior to reloading it.

HP Switch, Routing Switch, and Router Software Keys

Software Letter	HP Networking Products
A	Switch 2615-8-PoE and Switch 2915-8G-PoE
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.***xx*** and earlier
I	Switch 2800 Series (2824 and 2848)
J	**J.*xx.xx*.biz** Secure Router 7000dl Series (7102dl and 7203dl)
J	**J.*xx.xx*.swi** Switch 2520G Series (2520G-8-PoE, 2520G-24-PoE)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8212zl and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG).
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
P	Switch 1810G (1810G-8, 1810G-24)
PK	Switch 1810-48G
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
S	Switch 2520 Series (2520-8-PoE, 2520-24-PoE)
T	Switch 2900 Series (2900-24G and 2900-48G)
U	Switch 2510-48
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
W	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
WA	ProCurve Access Point 530
WM	ProCurve Access Point 10ag
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
Y	Switch 2510G Series (2510G-24 and 2510G-48)
Z	ProCurve 6120G/XG and 6120XG Blade Switches
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

OS/Web/Java Compatibility Table

The switch Web agent supports the following combinations of OS browsers and Java Virtual Machines:

Operating System	Internet Explorer	Java
Windows NT 4.0 SP6a	5.00, 5.01 5.01, SP1 6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.3.1.12 – Version 1.4.2.05
Windows 2000 Pro SP4	5.05, SP2 6.0, SP1	
Windows XP Pro SP2	6.0, SP2 and 7.0	Sun Java 2 Runtime Environment: – Version 1.5.0_11, Version 1.6.0
Windows Server SE 2003 SP2		
Windows Vista		

Minimum Software Versions

For HP Series 3500, 3500yl, 5400zl, 6200yl, 6600 and 8200zl Switches and Hardware Features

HP Device	Product Number	Minimum Supported Software Version
HP ProCurve 8206zl Switch Base System	J9475A	K.14.41
HP ProCurve 24-Port 10/100/1000 PoE+ zl Module	J9307A	K.14.41
HP ProCurve 20-Port 10/100/1000 PoE+/4-port MiniGBIC zl Module	J9308A	K.14.41
HP ProCurve 24-port 10/100 PoE+ zl Module	J9478A	K.14.41
HP ProCurve 5406zl-48G-PoE+ Switch	J9447A	K.14.41
HP ProCurve 5412zl-96G-PoE+ Switch	J9448A	K.14.41
HP ProCurve 10-GbE XFP-SFP+ 1m Direct Attach Cable	J9300A	K.14.37
HP ProCurve 10-GbE XFP-SFP+ 3m Direct Attach Cable	J9301A	K.14.37
HP ProCurve 10-GbE XFP-SFP+ 5m Direct Attach Cable	J9302A	K.14.37
HP ProCurve 10-GbE SFP+ 1m Cable	J9281B	K.14.32
HP ProCurve 10-GbE SFP+ 3m Cable	J9283B	K.14.32
HP ProCurve 10-GbE SFP+ 7m Cable	J9285B	K.14.32
HP ProCurve 3500-24 Switch	J9470A	K.14.31
HP ProCurve 3500-24-PoE Switch	J9471A	K.14.31
HP ProCurve 3500-48 Switch	J9472A	K.14.31
HP ProCurve 3500-48-PoE Switch	J9473A	K.14.31
HP ProCurve Switch 6600-48G	J9263A	K.14.24
HP ProCurve Switch 6600-48G-4XG	J9452A	K.14.24
HP ProCurve 10-GbE SFP+ 1m Cable	J9281A	K.14.03
HP ProCurve 10-GbE SFP+ 3m Cable	J9283A	K.14.03
HP ProCurve 10-GbE SFP+ 7m Cable	J9285A	K.14.03
HP ProCurve 10-GbE SFP+ SR Transceiver	J9150A	K.14.03

HP Device	Product Number	Minimum Supported Software Version
HP ProCurve 10-GbE SFP+ LR Transceiver	J9151A	K.14.03
HP ProCurve 10-GbE SFP+ LRM Transceiver	J9152A	K.14.03
HP ProCurve Switch 6600-24G	J9263A	K.14.03
HP ProCurve Switch 6600-24G-4XG	J9264A	K.14.03
HP ProCurve Switch 6600-24XG	J9265A	K.14.03
HP ProCurve ONE Services zl Module	J9154A	K.13.51
HP ProCurve 100-BX-D SFP-LC Transceiver	J9099B	K.13.45
HP ProCurve 100-BX-U SFP-LC Transceiver	J9100B	K.13.45
HP ProCurve 1000-BX-D SFP-LC Mini-GBIC	J9142B	K.13.45
HP ProCurve 1000-BX-U SFP-LC Mini-GBIC	J9143B	K.13.45
HP ProCurve 10-GbE X2-SC LRM Optic	J9144A	K.13.20
HP ProCurve Wireless Edge Services zl Module and the HP ProCurve Redundant Wireless Services zl Module	J9051A and J9052A	K.12.43
HP ProCurve Switch 8212zl Base System	J8715A	K.12.31
100-FX SFP-LC Transceiver	J9054B	K.12.01
Premium Features on Series 3500yl and 5400zl Switches	J8993A and J8994A	K.11.33
HP ProCurve Switch 5400zl 24p Mini-GBIC Module	J8706A	K.11.33
HP ProCurve Switch 5400zl 4p 10-GbE CX4 Module	J8708A	K.11.33
HP ProCurve Switch 6200yl-24G-mGBIC	J8992A	K.11.33
HP ProCurve Switch 3500yl 2p 10GbE X2 + 2p CX4 Module	J8694A	K.11.17
HP ProCurve Switch 8212zl Base system	J8715A/J8715B	K.12.31

Support Notes

ROM Update Required!

A successful update may require multiple steps, depending on your current software and boot ROM levels. Please see details in the table below.

If your software version is:	Your next step should be:
K.11.11 through K.12.29 (boot ROM K.11.00 - K.11.03)	Update and reload into software version K.12.62
K.12.31 through K.12.62 (boot ROM K.12.12)	Update and reload into software version K.13.49
K.13.49 or newer (confirm boot ROM K.12.14 or newer using 'show flash')	Update and reload directly into software version K.14.84
K.14 (any version)	

All 6600 and 3500 switches running K.14.69 or earlier system software will have the BootROM updated by this new version of system software. This software download will boot the switch **twice**, first to update the BootROM to version K.12.22, and then to load the system software. Following file copy to the switch flash and initiation of the reload, no additional user intervention is needed. **Do not interrupt power to the switch during this important update.**

To confirm that the boot ROM and system software have updated successfully following a reload into software version K.14.41 or newer, follow the process below at your switch CLI.

```
ProCurve_Switch# show flash

Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 9798890   08/27/09  K.14.41 <--Indicates that system software is updated
Secondary Image : 9524050   01/27/09  K.14.03
Boot Rom Version: K.12.20 <-- Indicates the boot ROM is updated
Default Boot    : Primary
```

Using SNMP To View and Configure Switch Authentication Features

Beginning with software release K.12.01, manager read/write access is available for a subset of the SNMP MIB objects for switch authentication (hpSwitchAuth) features. That is, in the default state, a device with management access to the switch can view the configuration for several authentication features, and using SNMP sets, can change elements of the authentication configuration.

Security Note In the default configuration for SNMP MIB object access, SNMP sets can be used to reconfigure password and key MIB objects. This means that a device operating as a management station with access to the switch can be used to change the SNMP MIB settings. This can pose a security risk if the feature is used to incorrectly configure authentication features or to reconfigure authentication features to unauthorized settings.

If you want to block the SNMP MIB object access described above, use the following command to disable the feature:

```
ProCurve(config)# snmp-server mib hpswitchauthmib excluded
```

For more information on the above topic, refer to “Using SNMP To View and Configure Switch Authentication Features” in the "RADIUS Authentication and Accounting" chapter of the *Access Security Guide* for your switch. For an overview of the security features available on the switch, refer to chapter 1, “Security Overview”, in the *Access Security Guide* for your switch.

Security:

Downloading and booting software release K.12.01 or greater for the first time automatically enables SNMP access to the hpSwitchAuth MIB objects. If this is not desirable for your network, ProCurve recommends that you disable it after downloading and rebooting with the latest switch software.

ACL numbering restrictions:

The K.12.01 release enforces ACL numbering restrictions.

See the Note under Version K.12.01 Software Fixes on page 168 (PR_1000389442) for details.

OSPF virtual link:

OSPF virtual links configurations will be lost with the update to K.12.01.

See the Note under Version K.12.01 Software Fixes on page 169 (PR_1000374003) for details.

MSTP auto-edge-port support and default settings:

With version K.12.04 (page 29), automatic detection of edge ports is supported, along with revised command options and default settings.

Resources (PR_1000388697):

When the switch is writing large files to flash (for example, a transfer of a very large configuration or a software update), switch resources may be impacted during the write operation, causing some potential loss of hello packets. This may impact VRRP, OSPF or spanning tree protocol. In order to mitigate potentially undesirable affects, updates to the switch software should be made during a scheduled downtime. Increasing the hello interval of time sensitive protocols may also assist with mitigation of this issue.

Support for the Wireless Edge Services zl Module

The addition of support for the zl Wireless Edge Services Module will change the way in which radio ports are treated by the zl and yl Series Switches. If the default setting of LLDP auto-provisioning is left intact, LLDP information from the ProCurve Radio Ports (J9004A, J9005A, J9006A) will trigger these devices to be placed into VLAN 2100 or the first available VLAN not already configured above that (see the section entitled Using Auto-Provisioning to Establish a Radio Port VLAN in the Management and Configuration Guide for ProCurve Wireless Edge Services zl Module here: ftp://ftp.hp.com/pub/networking/software/WESM-zl-MgmtCfg-Aug2007-59918626.pdf). Network administrators who do not wish to have the radio ports moved to the auto-provisioned VLAN should disable this feature with the command “no lldp auto-proision” at the CLI.

CAUTION: Updating to Version K.13.xx

It is important that you update to K.13.xx from a configuration that has not been previously converted from a pre-K.13.xx format (e.g. a K.11.xx or K.12.xx configuration). If you have previously updated to K.13.xx and rolled back to K.12.xx to workaround an issue, you should load a saved K.12.xx configuration to the switch and boot to it prior to updating to K.13 again.

Boot ROM requirement for K.14.xx

All switches must be running a boot ROM version of K.12.14 or newer in order to load K.14.xx software. (Note that all HP ProCurve 6600 Series Switches will ship with the required boot ROM version.) ProCurve 3500yl, 5400zl, 6200yl, and 8200zl switches will need to be updated and running software version K.13.49 or newer software before successfully loading K.14.xx software.

Please follow Best Practices for Major Software Updates (page 5) for configuration compatibility.

HP Security Policy and Release Notes

Per HP policy, a Security Bulletin must be the first published notification of a security defect. Fixes to security defects are not documented in release notes, also by HP policy. The official communication for security defect fixes will always be through HP Security Bulletins. For more information on security bulletins, and information on how to subscribe to them, please see **http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c02645131/c02645131.pdf**

Visit the HP networking web site for more information on security and HP Networking products:

http://h17007.www1.hp.com/us/en/solutions/security/index.aspx

Clarifications

The following clarification or updates apply to documentation for the ProCurve Series 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl Switches as of December 2009.

- **Maximum Number of VLANs Supported in Hardware for PIM-S —** Page 4-5 in the *Multicast and Routing Guide* dated January 2008 for switches running version K software incorrectly states that up to 2048 flows are supported in hardware across a maximum of 512 VLANs. Up to 2048 flows are supported across a maximum of 128 VLANs.

- **Maximum Number of Flows in the MRT —** Page 4-41 in the *Multicast and Routing Guide* dated January 2008 for switches running version K software incorrectly states that up to 1023 flows are supported. Up to 2048 flows are supported.

- **Enabling Jumbo Frames and Flow Control**:
  The Series 3500yl, 6200yl, 5400zl, and 8200zl switches support simultaneous use of Jumbo Frames and Flow Control. (An earlier version of the *Management and Configuration Guide* had incorrectly stated that these features could not be enabled at the same time.)

- **Clarification for the Number of IP addresses and maximum VLANs** that can be configured on the switch:

  You can configure a maximum of 512 routed VLANs per switch. A VLAN can be configured with up to 32 IP addresses. However, the maximum number of IP addresses that can be configured on the switch is 2048, so it is not possible to configure up to the maximum number of routed VLANs (512) with 32 IP addresses each. For example, if you wanted to use all available IP addresses for the switch and utilize all 512 possible routed VLANS with as many assigned IP addresses as possible, the configuration is calculated as follows:

  512 routed VLANs x 4 IP addresses per VLAN = 2048 total IP addresses.

  Refer to the *Advanced Traffic Management Guide* for further details.

- **TACACS+ Encryption Key Exclusion from TFTP Copies**
  When using the copy command to transfer a configuration to a TFTP server, any server-specific or global encryption keys in the TACACS+ configuration will not be included in the transferred file. Otherwise, a security breach could occur, allowing access to the TACACS+ user name/password information.

- **RIP and OSPF Redistribution:**
  RIP operation supports static, connected, and OSPF route redistribution. OSPF operation supports static, connected, and RIP route redistribution. (The earlier version of the *Advanced Traffic Management Guide* omitted RIP and OSPF route redistribution.)

- **Maximum UDP Broadcast Forwarding Entries:**
  The number of UDP broadcast entries and IP helper addresses combined can be up to 16 per VLAN, with an overall maximum of 2048 on the switch. An earlier version of the *Multicast and Routing Guide* (page 5-142) had incorrectly stated that the overall maximum is 256.

- **Reload Command Description**

  Syntax: **Reload**

  This command boots the switch from the currently active flash image and startup-config file. Because reload bypasses some subsystem self-tests, the switch boots faster than if you use a boot command. Note: To identify the currently active startup-config file, use the **show config files** command. (This is a clarification of *Syntax: Reload* (page 6.33) in the *Management and Configuration Guide.)*

  Using Reload

  The **reload** command reboots the switch from the flash image on which you are currently booted (primary or secondary) or the flash image that was set either by the **boot set-default** command or by the last executed **boot system flash** <***primary*** | ***secondary***> command. Because **reload** bypasses some subsystem self-tests, the switch reboots faster than when you use

either of the **boot** command options. If you are using redundant management and redundancy is enabled when using **reload**, the switch will failover to the other management module. (This is a clarification of *Using Reload* (page 6.24) in the *Management and Configuration Guide.)*

- **MSTP mCheck:**
  Unlike other MSTP parameters, 'mCheck' is not a configurable option. It is a flag that tells MSTP to initiate transmission of RST/MST BPDUs for a MigrateTime (3 secs) period, to test whether all STP Bridges on the attached LAN have been removed and the Port can migrate to the native MSTP mode and use RST/MST BPDUs for transmission. The 'mCheck' is always cleared (set FALSE) prior to port initialization. Some of the earlier ProCurve MSTP implementations allowed the 'mCheck' option to be a configurable parameter. It was stored in the config. That was corrected beginning with version K.12.04.

- **Virus-Throttling (Connection-rate filtering):** As of release K.12.01, this feature enables notification of worm-like behavior detected on all inbound IP traffic. (The Advanced Traffic Management Guide retains some incorrect references to filtering on IP routed traffic only.)

- **Menu Interface Configuration Limit:** The menu interface allows the user to perform VLAN port assignment for up to 32 VLANs. CLI or Web Management Interface should be used for VLAN port assignment beyond 32 VLANs.

- **IPv6**
  A valid IPv4 loopback address is required, as a minimum, for IPv6 addresses to be configured.

The following clarifications apply to documentation as of June 2009.

- **Virtual Stacking (3500yl/6200yl Series switches only)/Management VLANs:**
  A ProCurve switch that is configured as a Stack Member can no longer be managed by the Stack Commander if it is also configured with a Management VLAN. This is by design. The Management VLAN is configured when the network administrator desires an isolated, non-routable VLAN for use in managing the network. Virtual Stacking is intended to conserve IP addresses on the network by allowing the management of up to 16 Switches through the IP address of the Commander Switch. Due to the expectation that Stack Members will not have their own IP address, stacking traffic was not designed to traverse a Management VLAN. Virtual stacking and Management VLANs should therefore be considered mutually exclusive features.

- **Out of Band Management (OOBM) on 6600 Series switches/IPv6:**
  Beginning with software release K.14.42, IPv6 configuration of the OOBM interface is supported. Prior to release K.14.42, only IPv4 addresses were supported.

Known Issues

Release K.14.39

The following are known issues in release K.14.39 or newer. (K.14.39 is not a public release)

- **Premium Licensing (PR_0000043665)** — When telnet or SSH is used to communicate with the switch, hardware ID's that are reported by the switch in preparation as a prerequisite for premium license registration become truncated. Workaround: Console to the switch or use ProCurve Manager to obtain a valid hardware ID.

Release K.14.34

The following are known issues in release K.14.34 or newer.

- **Web Authentication (PR_0000041695)** — Web authentication for port-access does not function.
- **Config (PR_0000042930)** —The (fixed) "module " 1 which is usually present in the running and startup configurations is not present. Output from show run looks like the following.

  ```
  module 1 type
  module 2 type J86xxA
  ```

As a result, previously saved 3500yl configurations will not successfully upload to the switch. When attempts are made, it reports an error: `Invalid input: J86yyA`.

- **PoE+ (PR_0000039215)** — When a PoE+ port is connected to a PoE port (e.g., a switch-to-switch link), the PoE+ switch will sense that it is connected to Power Sourcing Equipment (PSE) and disable PoE on that port. Traffic will pass normally, and a message similar to the following will be seen in the event log. This is expected behavior.

  ```
  02562 port pp: PSE detected. Port PoE disabled
  ```

Once a port has had its PoE functionality disabled for this condition, the following steps may be used to recover PoE functionality on that port if the user wishes to connect it to a power device. A reboot will also recover functionality, but it is assumed the least disruptive solution is desired.

1. On the PoE-side of the connection, disable PoE power by using the CLI command **no power-over-ethernet [port-list]**.
2. On the PoE+ side of the connection, power down the module using the CLI command **savepower module [slot]**.
3. Power up the PoE+ module using the CLI command **no savepower module [slot]**.

- **CLI (PR_0000043262)** — The HP ProCurve Wireless Edge Services **zl** Module (J9051A) is incorrectly reported by the switch CLI as an **xl** module.
- **CLI (PR_0000041635)** — The CLI response to the **show modules** command always reports that a module is booting in response to the **no savepower module [slot]** command; there are times (for example, when the module was in an error state due to insufficient power to a 12-slot chassis) that the module will not initialize successfully without being re-seated or having the chassis rebooted.
- **8200zl Management Module Compatibility (PR_0000041133)** — When exchanging a management module from an 8212zl for use as the only management module in an 8206zl chassis (or vice versa), the management module must be on a boot ROM and software version that is supported by the 8206zl, and any existing configuration on the module must be erased after the module is inserted into the target switch (using the CLI command **erase startup-config**). The switch console should prompt the administrator to perform the necessary action after module insertion, but does not.

Release K.14.09

The following problems are known issues as of release K.14.09.

- **10-GbE (PR_0000038110)** — 10-GbE SFP+ transceivers may fail to form a stable link, and 10-GbE X2 transceivers may fail to initialize entirely or they may initialize only after a long delay.

Release K.14.03

The following problems are known issues as of release K.14.03.

- **CLI (PR_0000008236)** — The **enable** CLI command is listed in enable-mode help.
- **Config (PR_0000014381)** — Switches running K.14.03 or newer software may be unable to upload a valid config file to the switch, if it is set with the parameter, speed-duplex 1000-full, and on a dual personality port with a mini-GBIC inserted. The switch will display a message similar to the following. (The example below contained the speed-duplex value in line 8 of the config, and the value was applied to port 47.)

```
line: 8. Value 1000-full is not applicable to port 47.
Corrupted download file.
```

- **Config (PR_0000014818)** — Although the switch CLI provides an appropriate error message when the user tries to add more MAC addresses than a port is configured to allow, it seems to save the excess MAC addresses and display them in the configuration.
- **Syslog (PR_0000008241)** — Event log messages with a severity of "E" (error) are not always supported by default on syslog servers. The fix will update the **show logging** help text to clarify the dependency. In order to modify the syslog configuration file on a Linux server in order to receive error messages, complete the following steps.

  1. # vim /etc/syslog.conf
  2. Add the following line in the syslog.conf file:

     ```
     *.* /var/log/messages
     ```

  3. # /etc/init.d/syslog restart

- **Syslog (PR_0000012167)** — Syslog messages longer than 119 characters get truncated.
- **VRRP (PR_0000016192)** — In a VRRP topology with only VRRP Backups configured (i.e. there is no Master/Owner present in the setup), initializing the VRID(s) on both Backups at exactly the same time (e.g. after loss and restoration of power to all switches at once) can lead to a situation where both Backups will enter a continuous sequence of failovers.
- **IGMP (PR_0000009415)** — The switch may intermittently fail to forward a multicast stream.

Release K.13.51

The following problems are known issues as of release K.13.51.

- **Config (PR_0000014381)** — Switches running K.13.21 or newer software may not be able to upload a valid config file to the switch if it contains the parameter **speed-duplex 1000-full** on a dual personality port with a mini-GBIC inserted. The switch will provide the user with a message similar to the following (the example below contained the speed-duplex value in line 8 of the config, and the value was applied to port 47).

```
line: 8. Value 1000-full is not applicable to port 47.
Corrupted download file.
```

Release K.13.25

The following problems are known issues as of release K.13.25.

- **SFTP/SCP (PR_0000008270)** — An SFTP or SCP client session may not close after a config download session ends. The work-around is to close the client manually.

Release K.13.23

The following problems are known issues in release K.13.23 or newer.

- **MAC Authentication (PR_0000007477)** — When large numbers of MAC authentications are attempted immediately after the switch (re)boots, some of the MAC authentications may fail when they should succeed. Workaround: Increase the RADIUS server delay.

Release K.13.08

The following problems are known issues in release K.13.08 or newer.

- **CLI (PR_0000001893) —** The **copy flash** CLI command does not function in ProCurve 8212zl switches running K.13.05 or later. Workaround: use the CLI command **copy tftp flash**.
- **Config/TFTP (PR_1000748292)** — The switch allows conflicting configuration parameters to be loaded via TFTP transfer to the startup-config (**ip address** `<x.x.x.x>` and **no ip address**).
- **Port Security (PR_1000777162)** — When Port Security is configured for static MAC address learning, prolonged flooding of unicast traffic may occur under certain conditions.
- **Certificate (PR_1000416167)** — The Web Management interface submission form limits CA-signed certificates to 1800 bytes.
- **CLI (PR_1000760929)** — The CLI output from the command **show name int <x-x>** does not display the port number beyond the ninth port.
- **RADIUS/Jumbo (PR_ 1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **SNMP Trap (PR_1000772026)** — The ProCurve 3500yl Switches do not send the proper OID value for a Redundant Power Supply (RPS) failure.
- **Web (PR_1000761014)** — The Web interface truncates 16 character passwords to 15 characters. Workaround: configure 16 character passwords via the CLI.
- **ICMP (PR_1000764033)** — ICMP *TTL expired* messages are being sent with a source address of the interface the message leaves from rather than the interface that receives the expired packet.
- **Auto-TFTP/Config (PR_0000001410)** — Auto-TFTP configuration is lost during the update from K.12.xx to K.13.03.
- **Web Authentication (PR_0000000968)** — Web authentication to IAS over PEAP may trigger a software exception crash with a message similar to the following.

```
Software exception at exception.c:501 -- in 'mWebAuth', task ID = 0x843c2b0 -> internal
error
```

- **DHCP Snooping (PR_1000469934)** — When DHCP Snooping is enabled and configured, and a client sends a "DHCPINFORM" after receiving address information, the DHCP Server response is not forwarded to the client by the switch.
- **CLI (PR_1000745509)** — There are multiple issues with respect to the output from the CLI command **show ipv6 neighbor vlan <x>**.
- **Module Selftest (PR_0000001273)** — After reboot, ports 1-24 or ports 25-48 on the ProCurve 3500yl or ports 1-24 on the 6200yl Switches may become unresponsive followed by green and amber port LEDs remaining lit. Ports recover automatically. The log file will show the following messages.

```
chassis: Ports 1-24: Slave ROM Tombstone: 0x13000601
chassis: Ports 1-24: Lost Communications detected - Heart Beat Lost(4A)
chassis: Ports 1-24 Downloading
chassis: Ports 1-24 Download Complete
chassis: Ports 1-24 Ready
```

- **ECMP (PR_1000798467)** — A switch using OSPF ECMP may mis-route traffic for routes with long prefixes (/31 or /32).
- **CLI (PR_1000782972)** — The CLI command **show system power** provides incorrect output for those regions that use a 220 volt standard.
- **CLI (PR_1000430534)** — Output from the **show port-access mac-based** CLI command may omit connected clients.
- **CLI (PR_1000776583)** — The output for CLI command **show access-list resources** does not accurately display the number of QoS/ACL masks available.
- **Config Transfer (PR_1000781015)** — A config file transfer will fail with a "`corrupted configuration`" message, if the config file specifies MDIX-mode for a dual-personality port.
- **Config Transfer (PR_1000781004)** — The switch allows a config file transfer to set an invalid speed-duplex setting on a 100FX SFP.
- **Config Transfer (PR_1000781031)** — When the valid port setting 'auto-1000' is configured for a 10/100/1000 interface and the configuration gets copied to the switch, the port setting is altered to 'auto.'
- **Config Transfer (PR_1000781011)** — A config file copied to the switch allows an entry to enable flow control on a half-duplex interface. However, flow control on a half-duplex interface is disabled, as specified by IEEE 802.3 Annex 31B.
- **CLI (PR_1000775644)** — When flow control is enabled, the output from a **show int brief** CLI command inaccurately indicates that flow control is off.

Release K.13.02

The following are known issues in release K.13.02 or newer.

- **ACL Mirrors**: Beginning with K.13.02 software, ACLs can only be mirrored to a single destination.

Release K.13.01

The following are known issues in release K.13.01 or newer.

- **Rate-Limiting**: The "bps" mode for Ingress/Egress Rate-Limiting has been removed from the MIB, from the config, and as a CLI option (help-text also updated). Bandwidth is now measured in KBPS. Configurations which have rate-limiting configured in bps units will be successfully converted to the updated unit of measurement as the software is updated from K.11.xx or K.12.xx to K.13.xx.
- **PCM+ USB Autorun (PR_1000767612)** — Issuing the command copy startup-config usb test may crash the switch when executed in a PCM+ Autorun cmd file. The crash message is similar to:

  ```
  PPC Data Storage (Bus Error) exception vector 0x300:
  ```

- **Restriction in number of ACL mirror destinations** — The K.13.01 software introduced a new restriction to a single ACL mirror destination. K.12 versions of software allowed up to 4 ACL mirror destinations. Users with multiple ACL mirror sessions must edit their configurations so that they contain only a single mirror destination prior to updating to K.13.01 or newer software. If a switch with multiple ACL mirror destinations is updated from K.12.xx to K.13.01 or newer, only the first destination will function. The additional mirror sessions will have to be edited out of the configuration offline, and the valid configuration then loaded onto the switch.

Enhancements

This section lists only the software versions that contain enhancements. Enhancements are listed in chronological order, oldest to newest software release. Unless otherwise noted, each new release includes the enhancements added in all previous releases.

To review a summary of enhancements included since the last general release that was published, begin with "Release K.14.09 Enhancements" on page 60.

Descriptions and detailed instructions for enhancements included in Release K.13.01 or earlier are included in the latest release of manuals for the ProCurve Series 3500yl, 6200yl, 5400zl, and 8200zl switches (January 2008), available on the Web at **www.hp.com/rnd/support/manuals**.

Release K.11.11 was the first production software release for the ProCurve 3500yl, 6200yl, and 5400zl Series switches. Release K.12.31 was the first production software release for the ProCurve 8212zl switch. Release K.12.57 is the last public release of the K.12.*xx* software. The 3500yl, 6200yl, 5400zl, and 8212zl software code was rolled to the K.13.0*x* code branch with no intervening releases.

Release K.11.12 Enhancements

Release K.11.12 includes the following enhancement:

- MSTP Enhancement Implementation of legacy path cost MIB and CLI option for MSTP.

Release K.11.33 Enhancements

- With the K.11.33 software release, support for the following ProCurve products was added:
  - J8698A / J8700A(bundle) for the ProCurve switch 5412zl
  - J8706A - ProCurve Switch 5400zl 24p Mini-GBIC Module
  - J8708A - ProCurve Switch 5400zl 4p 10-GbE CX4 Module
  - J8992A - ProCurve Switch 6200yl-24G-mGBIC

Release K.11.34 Enhancements

Release K.11.34 includes the following enhancements:

- **Increased number of Telnet/SSH sessions**: The maximum number of simultaneous Telnet/SSH sessions has been increased from three to five. The CLI commands **show telnet** and **show ip ssh** now report on five sessions rather than just three.
- **CLI-configured sFlow with multiple instances:** In earlier software releases, the only method for configuring sFlow on the switch was via SNMP using only a single sFlow instance. Beginning with software release K.11.34, sFlow can also be configured via the CLI for up to three distinct sFlow instances. For more information, refer to the section on "CLI-Configured sFlow with Multiple Instances" in the chapter titled "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.
- **Event log display options**: Two new options have been added to provide greater flexibility in viewing event log entries via the CLI. The **show logging** command now includes an option to reverse the standard display, and a **clear logging** command has been added to remove all event log entries from the **show logging** display output. For more information, refer to the section on "Using the Event Log To Identify Problem Sources" in the Appendix titled "Troubleshooting" in the *Management and Configuration Guide* for your switch.

- **Scheduled reload:** Additional parameters have been added to the **reload** command to allow for a scheduled reboot of the switch via the CLI. For more information, refer to the section on "Rebooting your Switch" in the Chapter titled "Switch Memory and Configuration" in the *Management and Configuration Guide* for your switch.
- **Real-time rate display:** The **show interface port-utilization** command provides a real-time rate display for all ports on the switch.

Release K.11.35 Enhancements

Release K.11.35 includes the following enhancement:

- Added support for STP Per-Port BPDU Filtering and SNMP Traps.
- Added an option to configure the switch to use the management VLAN IP address in the Option 82 field for all DHCP requests received from various VLANs.

Release K.11.40 Enhancements

Release K.11.40 includes the following enhancement:

- **RSTP/MSTP BPDU Protection**: When this feature is enabled on a port, the switch will disable (drop the link) of a port that receives a spanning tree BPDU, log a message, and optionally, send an SNMP trap.

Release K.11.41 Enhancements

Release K.11.43 includes the following enhancement:

- Added support for Unidirectional Fiber Break Detection (UDLD).

Release K.11.43 Enhancements

Release K.11.43 includes the following enhancement:

- 802.1X Controlled Directions enhancement. With this change, Administrators can use "Wake-on-LAN" with computers that are connected to ports configured for 802.1X authentication.

Release K.11.44 Enhancements

Release K.11.44 includes the following enhancement:

- Loop Protection enhancement allows STP to detect and block network topology loops on a single port.

Release K.11.48 Enhancements

Release K.11.48 includes the following enhancement:

- The **show tech transceiver** CLI command output now contains the HP part number and revision information for all transceivers (mGBICs) on the switch.

Release K.11.49 Enhancements

Release K.11.49 includes the following enhancement:

- DHCP Protection (Snooping) enhancement.

Release K.11.64 Enhancements

Release K.11.64 includes the following enhancement:

- Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- Historical information about MAC addresses that have been moved has been added to the "show tech" command output.

Release K.11.68 Enhancements

Release K.11.68 includes the following enhancement:

- Improved SFlow function to accommodate bursty traffic.

Release K.11.69 is the last release of the K.11.*xx* software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.0*x* code branch with no intervening releases.

Release K.12.01 Enhancements

Syntax:Release K.12.01 is a major software update containing many new features and enhancements to existing features. The following updates have been documented in the latest revisions to the manuals (February 2007). Refer to the manuals for additional details.

Software Manual/ Enhancements	Description
Management and Configuration Guide	
Bi-directional Rate Limiting:	In earlier releases, all traffic rate-limiting applied to inbound traffic only, and was specified as a percentage of total bandwidth. This enhancement allows you to configure outbound rate-limiting for all traffic on a port, and specify bandwidth usage in terms of bits per second (bps).
Loopback Interface:	A virtual interface that is always up and reachable as long as at least one of the IP interfaces on the switch is operational. By default, each switch has an internal loopback interface (lo0). You can configure up to seven other loopback interfaces on the switch.
USB Support	Provides an option for using a USB device as a source or destination for file transfers. Refer to "Using USB To Download Switch Software" in the "File Transfers" appendix of the ***Management and Configuration Guide*** for your switch (February 2007 or newer). For information on USB device compatibility on the 3500yl, 5400zl, and 6200yl switches, refer to the HP networking support Website: **www.hp.com/networking/support**.
Intelligent Mirroring	Enables copying of network traffic from a network interface to a local or remote exit port where a host such as a traffic analyzer or intrusion detection system (IDS) is connected.
DNS Resolver	Used in local network domains to enable the use of a hostname or fully-qualified domain name to perform ping and traceroute operations from the switch.
SNMP-Server Source IP Commands:	Provides added security by allowing you to send SNMP replies from the same IP address as the one on which the corresponding SNMP request was received.
SNMPv3 AES Support:	Authentication and privacy for SNMPv3 users has been enhanced to support AES 128-bit encryption as a privacy protocol in SNMPv3 messages in compliance with RFC 3826.
Multicast and Routing Guide	
OSPF NSAA:	Support for Not-So-Stubby-Areas (NSAA).
DHCP Relay:	Enhancements to the DHCP Relay feature allow you to disable the hop count in DHCP requests, and enable support for up to 2048 IP helper addresses of DHCP servers.
Advanced Traffic Management Guide	
Qos Queue Config:	Allows you to reduce the number of outbound queues that all switch ports will use to buffer packets for 802.1p user priorities.
Number of Default VLANs:	In the factory default state, support has been increased from 8 VLANs to 256 VLANs. (You can reconfigure the switch to support up to 2048 (vids up to 4094) VLANs.)
Migrating Layer 3 VLANs Using VLAN MAC Configuration:	Allows you to upgrade to ProCurve routing switches without stopping the operation of attached hosts that use existing routers as their default gateway to route traffic between VLANs.
Access Security Guide	
RADIUS AAA:	Provides client-level security that allows LAN access to individual 802.1X clients (up to 32 per port), where each client gains access to the LAN by entering valid user credentials. This operation improves security by opening a given port only to individually authenticated clients, while simultaneously blocking access to the same port for clients that cannot be authenticated.
SNMP Access to Switch Authentication features:	Enables manager read/write access for a subset of the SNMP MIB objects for switch authentication features. **Security Note:** Downloading and booting software release K.12.01 or greater for the first time automatically enables SNMP access to the hpSwitchAuth MIB objects. For more information, or to disable this feature see"Support Notes" on page 14 for details.

Software Manual/ Enhancements	Description
Password Set via SNMP:	Allows configuration of username and password via SNMP.
Client-based Access Control:	In earlier releases, all traffic rate-limiting applied to inbound traffic only, and was specified as a percentage of total bandwidth. This enhancement allows you to configure outbound rate-limiting for all traffic on a port, and specify bandwidth usage in terms of bits per second (bps).
Virus Throttling on Bridged Traffic:	This enhancement allows connection-rate filtering on all IP traffic (not just routed traffic as in earlier releases).
ACLs on Port Traffic and Bridged Traffic:	Allows configuration of ACLs to filter traffic entering the switch on a VLAN or port.
Dynamic ARP Protection:	Protects your network from ARP cache poisoning by dropping packets, with an invalid IP-to-MAC address binding, that are received on untrusted ports.
Instrumentation Monitor:	Protects your network from a variety of common attacks by generating alerts for detected anomalies on the switch.
Controlled Directions Web/MAC Auth:	Allows you to use the aaa port-access controlled-directions command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state. This feature is available for both 802.1X and Web/MAC authorization.
Note on Manual Updates: In addition to the above updates to the manuals, the chapter on ACLs has been moved from the ***Advanced Traffic Management Guide*** to the ***Access Security Guide***. The ***Access Security Guide*** also provides a new introductory "Security Overview" chapter, plus a new chapter on "Advanced Threat Protection" covering topics such as DHCP Snooping and Dynamic Arp Protection.	

In addition to the updates listed above, K.12.01 also provides the following enhancements:

- **Enhancement (PR_1000298920)** — A ping request issued to a VLAN which is down will now return a more specific message; instead of "request timed out," the message "The destination address is unreachable" will be displayed.
- **Enhancement (PR_1000373226)** — Support was added for the ProCurve 100-FX SFP-LC Transceiver (J9054B).
- **Enhancement (PR_1000376626)** — Enhance CLI **qos dscp-map help** and **show dscp-map** text to warn the user that inbound classification based on DSCP code points only occurs if **qos type-of-service diff-services** is also configured.

Release K.12.03 Enhancements

Release K.12.03 includes the following enhancements:

- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the **show tech** command output.
- **Enhancement (PR_1000398393)** — For the **interface <*port-list*> speed-duplex** command, added the **auto-10-100** configuration option to constrain a link to 10/100 Mbps speed and allow a more rapid linkup process when 1000 Mbps operation is not possible.
- **Enhancement (PR_1000404544)** — Provides TCP/UDP port range prioritization in the **qos** command; the **range** option assigns an 802.1p priority to (IPv4) TCP or UDP packets associated with a range of TCP/UDP ports.

  qos <udp-port | tcp-port> < *tcp/udp port number* | range <*tcp/udp port number* > <*tcp/udp port number* > > priority < 0 - 7>

  For more information, refer to "QoS TCP/UDP Priority" in the *Advanced Traffic Management Guide*.

Release K.12.04 Enhancements

Release K.12.04 includes the following enhancement:

- **Enhancement MSTP (PR_1000369492)** — Update of MSTP implementation to the latest IEEE P802.1Q-REV/D5.0 specification to stay in compliance with the protocol evolution. For more information, refer to the *HP ProCurve Advanced Traffic Management Guide*.

Release K.12.05 Enhancements

Release K.12.05 includes the following enhancement:

- **Enhancement (PR_1000408960)** — RADIUS-Assigned GVRP VLANs enhancement. For more information, refer to the *HP ProCurve Access Security Guide*.

Release K.12.06 Enhancements

Release K.12.06 includes the following enhancement:

- **Enhancement (PR_1000308332)** — Passwords (hashed) can be saved to the configuration file. For more information, refer to the *HP ProCurve Access Security Guide*.

Release K.12.08 Enhancements

Release K.12.08 includes the following enhancement:

- **Enhancement (PR_1000413764)** — Increase the size of the sysLocation and sysContact entries from 48 to 255 characters.

Release K.12.10 Enhancements

Release K.12.10 includes the following enhancement:

- **Enhancement (PR_1000419653)** — The **show vlan ports** command was enhanced to display each port in the VLAN separately, display the friendly port name (if configured), and display the VLAN mode (tagged/untagged) for each port.

Release K.12.15 Enhancements

Release K.12.15 includes the following enhancement:

- **Enhancement (PR_1000427592)** — This enhancement adds the client's IP address to the RADIUS accounting packets sent to the RADIUS server by the switch.

  The IP address of the client is included in the RADIUS accounting packet sent by the switch to the RADIUS server. The client obtains the IP address through DHCP, so DHCP snooping must be enabled for the VLAN of which the client is a member.

- **Enhancement (PR_1000428642)** — The SNMP v2c describes two different notification-type PDUs: traps and informs. Prior to this software release, only the trap's sub-type was supported. This enhancement adds support for informs.

Release K.12.18 Enhancements

Release K.12.18 includes the following enhancement:

- **Enhancement (PR_1000428213)** — This software enhancement adds the ability to configure a secondary authentication method to be used when the RADIUS server is unavailable for the primary port access method. For more information, see the ProCurve *Access Security Guide*.
- **Enhancement (PR_1000415155)** — The ARP age timer was enhanced from the previous limit of 240 minutes to allow for configuration of values up to 1440 minutes (24 hours) or "infinite" (99,999,999 seconds or 3.2 years). For more information, see the ProCurve *Multicast and Routing Guide*.
- **Enhancement (PR_1000438015)** — The banner message of the day (MOTD) size has been increased to support up to 3070 characters.

Release K.12.21 Enhancements

Release K.12.21 includes the following enhancement:

- **Enhancement (PR_1000440049)** — Classifier-Based Rate Limiting capability was added. Classifier-Based Rate Limiting (also known as Rate Limit Port ACLs or RL-PACLs) allows you to create an ACL and apply it on a per-port basis to rate-limit network traffic. For more information, see the ProCurve *Access Security Guide*.
- **Enhancement (PR_1000374051)** — The 5400zl switches are not detecting packets from an Avaya G700 PBX or Cajun switch due to irregular Ethernet packets sent by those devices. This is a workaround that will alter the 5400zl software to allow 100Mb operation on the upcoming "C" revision of the 1000 Base-T Mini-GBICs (J8177C) that fit in the J8705A module. The port containing the 1000 Base-T Mini-GBIC can be configured with new speed options of "auto-100," "100-full," and "100-half."
- **Enhancement (PR_1000443349)** — This enhancement is to allow the concurrent use of SFTP with TACACS+ authentication for SSH connections. For more information, see the ProCurve *Access Security Guide*.

Release K.12.22 Enhancements

Release K.12.22 includes the following enhancement:

- **Enhancement (PR_1000443026)** — Support for the new revision "C" Mini-GBICs was added to the CLI and the "show tech" command.
- **Enhancement (PR_1000444415)** — OSPF Passive Interface support was added. For more information, see the ProCurve *Multicast and Routing Guide*.

Release K.12.23 Enhancements

Release K.12.23 includes the following enhancement:

- **Enhancement (PR_1000449129)** — This enhancement allows MAC or Web-based authentication to use PEAP/MS-CHAPv2 protocols in addition to the default setting of CHAP. For more information, see the ProCurve *Access Security Guide*.

Release K.12.31 Enhancements

Release K.12.31 includes the following enhancement:

- **Enhancement** — Support for the following ProCurve product was added.

  J9091A / J8715A (bundle) for the ProCurve switch 8212zl

Release K.12.32 Enhancements

Never released. Build K.12.32 includes the following enhancement:

- **Enhancement** — Merged all of the K.12.24 and earlier software fixes and enhancements with the ProCurve switch 8212zl support.

Release K.12.43 Enhancements

Release K.12.43 includes the following enhancement:

- **Enhancement** — Support for the following ProCurve products was added.

  J9051A ProCurve Wireless Edge Services zl Module

  J9052A ProCurve Redundant Wireless Edge Services zl Module

For more information, see "Support for the Wireless Edge Services zl Module" on page 15.

Release K.12.44 Enhancements

Release K.12.44 includes the following enhancement:

- **Enhancement (PR_1000457691)** — This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. (This enhancement was subsequently improved, see "Release K.12.51 Enhancements" on page 32.) For more information on MSTP VLANs, see the ProCurve *Advanced Traffic Management Guide*.
- **Enhancement (PR_1000457868)** — Local Proxy ARP enhancement. For more information, see the ProCurve *Multicast and Routing Guide*.
- **Enhancement (PR_1000456271)** — PC attached to telephone. (This enhancement was subsequently removed, see "Release K.12.47 Enhancements" on page 31.) For more information on endpoint device discovery, see the sections on LLDP-MED in the ProCurve *Management and Configuration Guide*. This enhancement was added back with Release K.12.51 (see "Release K.12.51 Enhancements" on page 32).

Release K.12.47 Enhancements

Release K.12.47 includes the following enhancement:

- **Enhancement Removed (PR_1000468258) —** The PC attached to IP telephone enhancement was removed.

Release K.12.48 Enhancements

Release K.12.48 includes the following enhancement:

- **Enhancement Removed (PR_1000470136) —** Removal of the enhancement that allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. The initial implementation of this enhancement did not allow smooth migration of pre-existing MSTP configurations. (For information on the initial implementation, see "Release K.12.44 Enhancements" on page 31. This enhancement was subsequently improved and re-introduced, see "Release K.12.51 Enhancements" on page 32.).

Release K.12.51 Enhancements

Release K.12.51 includes the following enhancements:

- **Enhancement (PR_10004570598) —** An improved version of the MSTP-VLAN mapping enhancement referenced in PR_1000457691 was added. This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. For more information, see the ProCurve *Management and Configuration Guide*.
- **Enhancement (PR_1000471015) —** Reintroduction of the feature referenced in PR_1000456271, that will allow a PC to connect with its RADIUS-assigned VLAN after an attached IP phone has authenticated on the authenticating port. For information on the initial implementation, see "Release K.12.44 Enhancements" on page 31.

Release K.12.52 Enhancements

Release K.12.52 includes the following enhancement (*Never Released.*):

- **Enhancement (PR_1000458484) —** This enhancement allows the user to set a maximum frame size for jumbo frames at the global level. For more information, see the ProCurve *Management and Configuration Guide*.
- **Enhancement (PR_1000461576) —** This enhancement introduces PVST Protection and Filtering. For more information, see the ProCurve *Advanced Traffic Management Guide*.
- **Enhancement (PR_1000462841) —** This enhancement changes the re-authentication process to allow an authenticated client to remain authenticated during re-authentication. For more information, see the ProCurve *Access Security Guide*.
- **Enhancement (PR_1000462104) —** This enhancement allows the configuration of modules not currently inserted in the switch. For more information, see the ProCurve *Management and Configuration Guide*.
- **Enhancement (PR_1000462847) —** This enhancement allows the configuration of transceivers not currently inserted in the switch. For more information, see the ProCurve *Management and Configuration Guide*.

Release K.12.56 Enhancements

Release K.12.56 includes the following enhancement:

- **Enhancement (PR_1000464170) —** This feature provides support for adding the LLDP VLAN Name TLV to LLDP advertisements generated by HP switches.

Release K.12.57 Enhancements

Release K.12.57 includes the following enhancement:

- **Enhancement (PR_1000713394) —** Adjustable IGMP Querier interval.

Release K.12.57 is the last public release of the K.12.*xx* software. The series 3500yl, 6200yl, 5400zl, and 8212zl switches software code was rolled to the K.13.0*x* code branch with no intervening releases.

Release K.13.01 Enhancements

Release K.13.01 is a major software update containing many new features and enhancements to existing features, including IPv6 host and application layer features (see "IPv6 Configuration Guide for 2900/3500/5400/6200/8200" on page 34 for details).

The following enhancements have been documented in the latest revisions to the manuals (January 2008). Refer to the indicated manuals for additional details.

Software Manual/ Enhancements	Description
Management and Configuration Guide	
PoE Power Allocation Methods:	Allows you to manually allocate the amount of PoE power for a port by either its class or a defined value.
USB Secure Autorun:	Helps ease the configuration of ProCurve switches by providing a way to auto-execute CLI commands from a USB flash drive. Note that the ability to create a valid AutoRun file also requires ProCurve Manager. For details, see the section on "USB Autorun" in the Appendix on "File Transfers".
SNMP Traps:	Allow you to configure the switch to send network security and link-change notifications to configured trap receivers. More error conditions can be reported and logged to help resolve security threats and network issues.
MAC-based Remote Mirroring:	Allows you to use MAC as a criteria in selecting traffic that needs to be monitored in addition to current port, ACL, and direction criteria.
Show Command Changes:	The **show power-management** CLI command has been changed to **show power-over-ethernet**. You can use this command and the **show power slot <slot-id>** to display information about PoE power. The **show system-information** CLI command syntax has been changed to **show system** with additional options to display details of system components: **fans**, **information**, **power-supply**, and **temperature**.
Scalability:	Increased max trunks (60); and increased helper address (4k). For scalability values for VLANs, hardware, ARP, and routing, see the new Appendix titled "Scalability: IP Address, VLAN, and Routing Maximum Values".
Advanced Traffic Management Guide	
STP Root Guard:	STP root guard allows user to prevent changes to the root bridge and thus preventing malicious attackers from modifying the root switch and ensuring that the STP topology maintain the optimal setting.
QinQ:	QinQ (provider bridging) has been added to allow frames from multiple customers to be forwarded through another topology (provider network) using service VLANs or S-VLANs. For more information, see the new "QinQ Provider Bridging" chapter.
STP Diagnostics:	Adds more diagnostic functions to resolve STP issues. See the section on "Troubleshooting an MSTP configuration" in the chapter on Multiple Instance Spanning-Tree Operation.
Routing and Multicast Guide	
Host-based OSPF-ECMP:	Allows OSPF to add routes with multiple next-hop addresses and with equal costs to a given destination IP address.

Software Manual/ Enhancements	Description
Access and Security Guide	
Dynamic Configuration Arbiter:	ProCurve provides different methods (for example, CLI, SNMP, or IDM/RADIUS) to configure network and security parameters and respond to threats. This feature allows you to determine the client-specific parameters that are assigned in an authentication session by applying or removing them as needed in a specified hierarchy of precedence.
RADIUS Attributes:	Additional RADIUS attributes included with this release: • Change of authorization: allows changes to user service without re-authentication • Vendor-ID: allows Microsoft RADIUS servers to use vendor ID as part of the policy • Capability advertisement: allows the switch to advertise its capability to the RADIUS server • Session termination: allows the switch to report to the RADIUS server the reason a session is terminated For more information, see the section on "Additional RADIUS Attributes" in the chapter on "RADIUS Authentication and Accounting".
RADIUS VLAN Support:	Supports RADIUS-assigned tagged and untagged VLAN configuration on an authenticated port. This allows you, for example, to use IDM to dynamically configure tagged and untagged VLANs as required for different client devices, such as PCs and IP phones, that share the same switch port. See the section on "VLAN Assignment in an Authentication Session" in the chapter on "RADIUS Authentication and Accounting".
PoE Planning and Implementation Guide	
Power Redundancy:	Support has been added for PoE redundancy. When PoE redundancy is enabled, PoE redundancy occurs automatically. The switch keeps track of power use and won't supply PoE power to additional PoE devices trying to connect if that results in the switch not having enough power in reserve for redundancy if one of the power supplies should fail.

Note on Manual Updates:

In addition to the above updates to the manuals, with this release the 8212zl software manuals and 3500/5400/6200 software manuals have been combined into a single manual set. Where features apply only to a specific model or models, this will be indicated in the chapter or heading for that feature; for example, "Redundancy (Switch 8212zl)" or "Stack Management for the Series 3500yl Switches and the 6200yl Switch."

New Product Documentation:

IPv6 Configuration Guide for 2900/3500/5400/6200/8200. Provides background information on IPv6 technologies and concepts, plus complete coverage of ProCurve's implementation of CLI commands for configuring IPv6 host and application layer features, including IPv6 addressing, auto configuration, dual stack support (IPv4/IPv6), Multicast Listener Discovery (MLD), IPv6 management and diagnostics.

The *Master Index* is a new feature to help find information more readily, providing clickable links from a combined Master Index PDF to the per Chapter PDF files from all five software manuals. To locate and access topics across the combined manual set using the index, download the Master Index zip file from the Web to a directory on your computer.

Release K.13.02 Enhancements

Release K.13.02 includes the following enhancements.

- **Enhancement**: Beginning with K.13.02, DHCP can now be enabled on a Management VLAN. Since, by definition, there is no routing to or from a VLAN configured as a management VLAN, DHCP relay is still prohibited so the DHCP server must be attached to the management VLAN for that VLAN to acquire an address. All DHCP options will be supported.

- **Enhancement (PR_1000458124) —** VRRP Preemptive Delay Timer. For more information, see the *HP ProCurve MultiCast and Routing Guide*, chapter 6.

Release K.13.03 Enhancements

Release K.13.03 includes the following enhancements.

- **Enhancement (PR_1000400991) —** The 802.1X Controlled Directions feature now functions independently of the STP configuration, allowing you to run STP and 802.1X separately. New commands are covered in the *HP ProCurve Access Security Guide*, chapter13.

Release K.13.04 Enhancements

Release K.13.04 includes the following enhancements.

- **Enhancement (PR_ 0000000081) —** The CLI **clear module** command allows you to remove module configuration information from the configuration file. For more information, see the *HP ProCurve Management and Configuration Guide*, chapter 10.
- **Enhancement (PR_ 0000000082) —** The CLI **track interface** command allows you to configure tracking for a port or list of ports, or a trunk or list of trunks. For more information, see the *HP ProCurve Multicast and Routing Guide*, chapter 6.
- **Enhancement (PR_ 0000000084) —** DHCP Option 66 provides a way to automatically download and initially boot from a configuration that is different from the factory-shipped configuration. For more information, see the *HP ProCurve Management and Configuration Guide*, chapter 6.
- **Enhancement (PR_ 0000000085) —** The DHCP relay address configuration enhancement provides a way to configure a gateway address for the DHCP relay agent to use for DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address. For more information, see the *HP ProCurve Multicast and Routing Guide*, chapter 5.
- **Enhancement (PR_ 0000000086) —** This enhancement allows rate-limiting of inbound broadcast and multicast traffic on the switch. For more information, see the *HP ProCurve Management and Configuration Guide*, chapter 13.
- **Enhancement (PR_ 0000000087) —** This enhancement enables a Telnet client to use the histamine in command input. For more information, see the *HP ProCurve Management and Configuration Guide*, chapter 7.
- **Enhancement (PR_ 0000000089) —** The CLI **show modules** command displays additional component information for system support modules and mini-GBICS. For more information, see the *HP ProCurve Management and Configuration Guide*, chapter 15 and appendix B.
- **Enhancement (PR_ 0000000101) —** This enhancement adds a **vrrp** option to the **debug** command. For more information, see the *HP ProCurve Multicast and Routing Guide*, chapter 6.
- **Enhancement (PR_ 0000000420) —** This enhancement provides the **show-tech** option for customizing **copy tftp** output. For more information, see the *HP ProCurve Management and Configuration Guide*, chapter 1.

Release K.13.16 Enhancements

Release K.13.16 includes the following enhancements:

- **Enhancement (PR_0000001641)** — This enhancement allows the user to set the console inactivity time out without rebooting the switch.

Console/Telnet Inactivity Timer

This enhancement allows you to configure the inactivity timer and have the new value take effect immediately, without a reboot of the system.

Syntax: console inactivity-timer <minutes>

If the console port has no activity for the number of minutes configured, the switch terminates the session. A value of zero indicates the inactivity timer is disabled.

Default: 0 (zero)

For example:

```
ProCurve(config)# console inactivity-timer 20
```

- **Enhancement (PR_1000780247)** — This enhancement provides hpicf Download MIB support for transferring configuration files both to and from a TFTP server. Prior to this enhancement, MIB support was limited to downloading and uploading software files.
- **Enhancement (PR_0000001430)** — This enhancement allows the user to configure access methods for IP Authorized Manager entries. For more information, see the *HP ProCurve Management and Configuration Guide*, chapter 3.
- **Enhancement (PR_0000000090)** — This enhancement allows you to choose which information to display when you enter the **show interfaces** command. For more information, see the *HP ProCurve Advanced Traffic Management Guide*, chapter 1.
- **Enhancement (PR_0000000857)** — This enhancement reduces the PIM delay time, thereby reducing the amount of time it takes for a packet to arrive at its destination when an IGMP Join is issued. A delay occurs in PIM when processing IGMP Join messages. This enhancement reduces the delay, thereby reducing the amount of time it takes for a packet to arrive at its destination when an IGMP Join is issued. There are no CLI changes with this enhancement.
- **Enhancement (PR_0000001790)** — This enhancement provides the **no-tag-added** parameter that gives the user the option of not tagging a mirrored copy of an outbound packet. For more information, see the *HP ProCurve Advanced Traffic Management Guide*, chapter 2.
- **Enhancement (PR_1000756562)** — This enhancement provides concurrent Web/MAC and 802.1x authentication. For more information, see the *HP ProCurve Access Security Guide*, chapter 4.
- **Enhancement (PR_0000000088)** — This enhancement provides new features for use with SSH. The SSH enhancements are: AES encryption (included in the K.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection; A configurable key; Message Authentication Code (MAC) configuration. A new configuration option provides the ability to configure which MACs a client is permitted to use; Feedback information; and, SSH CLI **show** command information enhancements.

SSH Enhancements

Overview

The SSH enhancements are:

- AES encryption (included in the K.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection.
- Configurable key

- Message Authentication Code (MAC) configuration. A new configuration option provides the ability to configure which MACs a client is permitted to use.
- Feedback information
- SSH CLI **show** command information enhancements

Specifying the Set of Ciphers

The following command allows you to specific which ciphers are available for a client to use for connection. All ciphers are available by default; use the **no** form of the command to disable specific ciphers.

Syntax: [no] ip ssh [cipher <cipher-type>]

Cipher types that can be used for connection by clients. Valid types are:

- *aes128-cbc*
- *3des-cbc*
- *aes192-cbc*
- *aes256-cbc*
- *rijndael-cbc@lysator.liu.se*
- *aes128-ctr*
- *aes192-ctr*
- *aes256-ctr*

Default: All cipher types are available.

Use the **no** *form of the command to disable a cipher type.*

```
ProCurve(config)# no ip ssh cipher 3des-cbc
```

Figure 1. Example of Disabling a Specific Cipher

Configuring Key Lengths and DSA/RSA Support

This enhancement allows you to specify the type and length of the generated host key. The command is:

Syntax: crypto key generate ssh [dsa | rsa [bits <num-bits>]]

Specify the type and length of the host key that is generated.

You can also generate and use a DSA key as the host key. The size of the host key is platform- dependent as different switches have different amounts of processing power. The size is represented by the *<num-bits>* key word and has the values shown in Table 1. The default value is used if **num-bits** is not specified.

Table 1. RSA/DSA Values for Various ProCurve Switches

Platform	Maximum RSA Key Size (in bits)	DSA Key Size (in bits)
5400/3500/6200/8200/2900	1024, 2048, 3072 Default: 2048	1024
2610	1024, 2048 Default: 1024	1024

Message Authentication Code (MAC) Support

This enhancement allows configuration of the set of MACs that are available for selection.

Syntax: [no] ip ssh [mac <MAC-type>]

Allows configuration of the set of MACs that can be selected. Valid types are:

- *hmac-md5*
- *hmac-sha1*
- *hmac-sha1-96*
- *hmac-md5-96*

Default: All MAC types are available.

Use the **no** *form of the command to disable a MAC type.*

Displaying the SSH Information

The **show ip ssh** command has been enhanced to display information about ciphers, MACs, and key types and sizes.

```
ProCurve(config)# show ip ssh

  SSH Enabled     : No                  Secure Copy Enabled : No
  TCP Port Number : 22                  Timeout (sec)       : 120
  IP Version      : IPv4orIPv6
  Host Key Type   : RSA                 Host Key Size       : 1024

  Ciphers : aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc,
            rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
  MACs    : hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96

  Ses Type     | Source IP                                        Port
  --- -------- + ------------------------------------------------ -----
  1   console  |
  2   inactive |
  3   inactive |
  4   inactive |
  5   inactive |
  6   inactive |
```

Figure 2. Example of show ip ssh Command Showing Ciphers, MACs and Key Information

Logging Messages

There are new event log messages when a new key is generated and zeroized for the server:

ssh: New <num-bits> -bit [rsa | dsa] SSH host key installed
ssh: SSH host key zeroized

There are also new messages that indicates when a client public key is installed or removed:

ssh: <num-bits>-bit [rsa | dsa] client public key [installed | removed] ([manager| operator] access) (key_comment)
Note: Only up to 39 characters of the key comment are included in the event log message.

Debug Logging

To add ssh messages to the debug log output, enter this command:

```
ProCurve# debug ssh LOGLEVEL
```

where LOGLEVEL is one of the following (in order of increasing verbosity):

- fatal
- error
- info
- verbose
- debug
- debug2
- debug3

Release K.13.18 Enhancements

Release K.13.18 includes the following enhancements:

- **Enhancement (PR_1000406763)** — New commands were added to the CLI response to the **show tech** command.

Release K.13.19 Enhancements

Release K.13.19 includes the following enhancements:

- **Enhancement (PR_0000003808)** — This enhancement allows the user to create command aliases for use in place of command names and their options. For more information, see the *HP ProCurve Management and Configuration Guide*, chapter 4.
- **Enhancement (PR_0000000818)** — This enhancement allows the user to enter addresses and filter parameters for syslog using SNMP, which allows more options for remote access and management of the switch. For more information, see the *HP ProCurve Management and Configuration Guide*, appendix C.
- **Enhancement (PR_0000003390)** — This enhancement allows the user to customize Web Authentication HTML pages. For more information, see the *HP ProCurve Access Security Guide*, chapter 4.

  Enhancement (PR_1000460265) — This enhancement provides Dynamic IP Lockdown, which is used to prevent IP source address spoofing on a per-port and per-VLAN basis. For more information, see the *HP ProCurve Access Security Guide*, chapter 11.

Release K.13.20 Enhancements

Release K.13.20 includes the following enhancements:

- **Enhancement (PR_0000004124)** — Support is added for the J9144A ProCurve 10-GbE X2-SC LRM Optic, an X2 form-factor transceiver that supports the 10-Gigabit LRM standard, providing 10-gigabit connectivity for up to 220 meters on legacy multimode fiber.

Release K.13.40 Enhancements

Release K.13.40 includes the following enhancements (Never released):

- **Enhancement (PR_0000003127)** — Link Trap and LACP Global Enable/Disable.

LACP and Link Traps Global Disable

Two SNMP commands are added to allow disabling of LACP and link traps on multiple ports at one time. The new commands operate in the same manner as the CLI commands **no int all lacp** and **no snmp-server enable traps link-change all**.

The new SNMP OIDs are:

```
hpSwitchLACPConfig OBJECT IDENTIFIER ::= { hpSwitchConfig 28 }

hpSwitchLACPAllPortsStatus OBJECT-TYPE
      SYNTAX INTEGER {

                                    disabled (1),
                                    active (2),
                                    passive (3)

                               }

      ACCESS  read-write
      STATUS  mandatory
       DESCRIPTION “Used to set administrative status of LACP on all the
                    ports. A Port can have one of the three
                    administrative status of LACP.
                    Active/Passive/Disabled are the three states.”
      ::= { hpSwitchLACPConfig 1 }

hpSwitchLinkUpDownTrapAllPortsStatus OBJECT-TYPE
      SYNTAX INTEGER {
                                    enable (1),
                                    disable (2)
                               }
      ACCESS  read-write
      STATUS current
      DESCRIPTION “Used to either enable/disable the Link Up/Link Down traps
                for all the ports.”
      ::= { hpSwitchPortConfig 3 }
```

- **Enhancement (PR_0000003128)** — The ability to clear statistics was added.

Clear Statistics Without Reboot

It is useful to be able to clear all counters and statistics without rebooting the switch when troubleshooting network issues. The **clear statistics global** command clears all counters and statistics for all interfaces except SNMP. You can also clear the counters and statistics for an individual port using the **clear statistics <*port-list*>** command.

Syntax: clear statistics <<***port-list***> | global >

When executed with the **<*port-list*>** *option, clears the counters and statistics for an individual port. When executed with the* **global** *option, clears all counters and statistics for all interfaces except SNMP.*

The **show interfaces [<*port-list*>]** command displays the totals accumulated since the last boot or the last **clear statistics** command was executed. The menu and web pages also display these totals.

SNMP displays the counter and statistics totals accumulated since the last reboot; it is not affected by the **clear statistics global** command or the **clear statistics <*port-list*>** command. An SNMP trap is sent whenever the statistics are cleared.

Note The clearing of statistics cannot be uncleared.

- **Enhancement (PR_0000003718)** — The MAC Lockout limit was increased.

Increase MAC Lockout to 64

The MAC lockout feature allows all traffic to or from a given MAC address to be dropped by the switch. A MAC address can exist on many different VLANs, so a lockout MAC address must be added to the MAC table as a drop. As this can quickly fill the MAC table, restrictions are placed on the number of lockout MAC addresses based on the number of VLANs configured. The restriction for the range of 17-256 VLANs is being increased to allow up to 64 lockout MAC addresses.

VLANs Configured	Number of MAC Lockout Addresses	Total Number of MAC Addresses
1-8	200	1,600
9-16	100	1,600
17-256	**64**	**16,384**
257-1024	16	16,384
1025-2048	8	16,384

- **Enhancement (PR_0000007388)** — Crash Log Debug was enhanced. For more information, see the *HP ProCurve Management and Configuration Guide*, appendix C.

Release K.13.43 Enhancements

Release K.13.43 includes the following enhancements (Not a public release):

- **Enhancement (PR_0000003557)** — The ability to enable/disable the USB port via CLI and SNMP was added. Note that after being disabled and subsequently re-enabled, the USB port may not function consistently with the PCM USB Autorun features until the switch has been reloaded.

USB Port Config via CLI and SNMP

CLI Implementation

This feature allows configuration of the USB port with either the CLI or SNMP.

To enable/disable the USB port with the CLI:

Syntax: usb-port
no usb-port

Enables the USB port. The **no** *form of the command disables the USB port.*

To display the status of the USB port:

Syntax: show usb-port

Displays the status of the USB port. It can be enabled, disabled, or not present.

```
ProCurve(config)# show usb-port

  USB port status: enabled
```

Figure 3. Example of show usb-port Command Output

SNMP Implementation

The HP enterprise MIB hpicfUSBPort.mib allows configuration of the USB port with SNMP.

```
HP-ICF-USBPORT DEFINITIONS ::= BEGIN

  IMPORTS
     OBJECT-TYPE, MODULE-IDENTITY
        FROM SNMPv2-SMI
     TruthValue
        FROM SNMPv2-TC
     hpSwitch
        FROM HP-ICF-OID;

  hpicfUSBPortMIB MODULE-IDENTITY
     LAST-UPDATED "200806250000Z"
     ORGANIZATION "Hewlett-Packard Company,
                   Workgroup Networks Division"
     CONTACT-INFO "Hewlett Packard Company
                   8000 Foothills Blvd.
                   Roseville, CA 95747"
     DESCRIPTION "This MIB module manages the USB Port.”
     ::= { hpSwitch 53 }
```

```
-- USBPort Configuration

hpicfUSBPortConfig    OBJECT IDENTIFIER ::= { hpicfUSBPortMIB 1 }

hpicfUSBPortStatus OBJECT-TYPE
   SYNTAX      INTEGER {
                    notPresent(0),
                    enabled(1),
                    disabled(2) }

   MAX-ACCESS  read-write
   STATUS      current
   DESCRIPTION "hpicfUSBPortStatus control whether of not
                the USB port is enabled.
                   notPresent(0)  - USBPort is not present
                   enabled(1)  - USBPort Enabled.
                   disabled(2) - USBPort Disabled."
   DEFVAL { enabled }
   ::= { hpicfUSBPortConfig 1 }

-- USBPort conformance information

hpicfUSBPortConformance
  OBJECT IDENTIFIER ::= { hpicfUSBPortMIB 2 }

hpicfUSBPortGroups
  OBJECT IDENTIFIER ::= { hpicfUSBPortConformance 1 }

hpicfUSBPortBaseGroup OBJECT-GROUP
   OBJECTS     {
                hpicfUSBPortStatus
               }
   STATUS      current
   DESCRIPTION "A mandatory group with an object to enable
                or disable the USB port."
   ::= { hpicfUSBPortGroups 1 }

-- USBPort conformance statements

hpicfUSBPortCompliances
   OBJECT IDENTIFIER ::= { hpicfUSBPortConformance 2 }

hpicfUSBPortCompliance MODULE-COMPLIANCE
   STATUS      current
   DESCRIPTION "Compliance statement for HP ICF USBPort
                configuration"
   MODULE
      MANDATORY-GROUPS { hpicfUSBPortBaseGroup }
   ::= { hpicfUSBPortCompliances 1 }



END
```

Release K.13.45 Enhancements

Release K.13.45 includes the following enhancements.

- **Enhancement (PR_0000010783)** — Support was added for the following products.

  J9099B - ProCurve 100-BX-D SFP-LC Transceiver

  J9100B - ProCurve 100-BX-U SFP-LC Transceiver

J9142B - ProCurve 1000-BX-D SFP-LC Mini-GBIC

J9143B – ProCurve 1000-BX-U SFP-LC Mini-GBIC

Release K.13.51 Enhancements

Release K.13.51 includes the following enhancements.

- **Enhancement** – Support is added for the J9154A HP ProCurve ONE Services zl Module.
- **Enhancement (PR_0000003144)** — Support is added for multiple RADIUS groups.

RADIUS Server Groups

Overview. The authentication and accounting features on the switch can use up to three RADIUS servers, a primary server and two backup servers. This feature allow the RADIUS servers to be put into a group. The same three RADIUS servers would continue to be used. Up to 5 groups of RADIUS servers can be configured. The authentication and accounting features can choose which RADIUS server group to communicate with. End-user authentication methods (802.1X, MAC-based and web-based) can authenticate with different RADIUS servers from the management interface authentication methods (console, telnet, ssh, web).

Commands Used. Several commands are used to support the RADIUS server group feature. The RADIUS server must be configured before it can be added to a group. See "RADIUS Authentication and Accounting" in the *Access Security Guide* for your switch for more information on configuring RADIUS servers.

Syntax: [no] radius-server host < ***ip-address*** >

Adds a server to the RADIUS configuration or (with **no***) deletes a server from the configuration. You can configure up to three RADIUS server addresses. The switch uses the first server it successfully accesses.*

Syntax: aaa server-group radius <***group-name***> host <***ip-addr***>
no aaa server-group radius <***group-name***> host <***ip-addr***>

Associates a RADIUS server with a server group.
The **no** *form of the command removes the RADIUS server with the indicated IP address from the server group. If that server was the last entry in the group, the group is removed.*

radius <group-name>*: The group name of the RADIUS server group. The name has a maximum length of 12 characters. Up to five groups can be configured with a a maximum of three RADIUS servers in each group. The first group slot is used by the default group.*

host <*ip-addr*>*: The IP address of the RADIUS server to be used.*

Enhanced Commands

The following commands have the **server-group** option. If no **server-group** is specified, the default RADIUS group is used. The server group must have already been configured.

Note The last RADIUS server in a server group cannot be deleted if an authentication or accounting method is using the server group.

Syntax: aaa authentication <console | telnet | ssh | web> < enable | login <local | radius [server-group <***group-name***> | local | none | authorized]>>

Configures the primary password authentication method for console, Telnet, SSH, and/or the web browser interface.

<**enable | login**>: *Primary authentication method. Default: local*

<**local | radius**>*: Use either the local switch user/password database or a RADIUS server for authentication.*

<**server-group <group-name>**>*: Specifies the server group to use.*

[local | none | authorized]: *Provides options for secondary authentication (default:* **none***). Note that for console access, secondary authentication must be* **local** *if primary access is not* **local***. This prevents you from being locked out of the switch in the event of a failure in other access methods.*

Syntax: aaa authentication <port-access <local |eap-radius | chap-radius> | <mac-based | web-based <chap-radius | peap-mschapv2> [none | authorized | server-group <***group-name***>] >>

Configures the primary authentication method for port-access, MAC-based, or web-based access.

mac-based | web-based <chap-radius | peap-mschapv2>*: Password authentication for web-based or MAC-based port access to the switch. Use* **peap-mschapv2** *when you want password verification without requiring access to a plain text password; it is more secure. Default:* **chap-radius**

port-access <local |eap-radius | chap-radius>*: Configures* **local**, **chap-radius (**MD5**)**, *or* **eap-radius** *as the primary password authentication method for port-access. The default primary authentication is* **local**. *(Refer to the documentation for your RADIUS server application.)*

[**none | authorized | server-group <group-name**>]*:*
none*: No backup authentication method is used.*
authorized*: Allow access without authentication*
server-group <group-name>*: Specifies the server group to use with RADIUS.*

Syntax: aaa accounting <exec | network | system | commands | <start-stop | stop-only>
radius [server-group <***group-name***>]

Configures accounting type and how data will be sent to the RADIUS server.

radius*: Uses RADIUS protocol as accounting method.*

server-group <group-name>*: Specifies the server group to use with RADIUS.*

Displaying the Server Group Information. The **show server-group radius** command displays the same information as the **show radius** command, but displays the servers in their server groups.

```
ProCurve(config)# show server-group radius

 Status and Counters - AAA Server Groups

  Group Name: radius

                  Auth  Acct  DM/  Time
  Server IP Addr  Port  Port  CoA  Window  Encryption Key
  --------------- ----- ----- ---- ------- --------------------------------
  192.168.1.3     1812  1813  No   300     default_key
  192.168.3.3     1812  1813  No   300     grp2_key
  192.172.4.5     1812  1813  No   300     grp2_key
  192.173.6.7     1812  1813  No   300     grp2_key
  192.168.30.3    1812  1813  No   300     grp3_key
  192.172.40.5    1812  1813  No   300     grp3_key
  192.173.60.7    1812  1813  No   300     grp3_key

Group Name: group2
                  Auth  Acct  DM/  Time
  Server IP Addr  Port  Port  CoA  Window  Encryption Key
  --------------- ----- ----- ---- ------- --------------------------------
  192.168.3.3     1812  1813  No   300     grp2_key
  192.172.4.5     1812  1813  No   300     grp2_key
  192.173.6.7     1812  1813  No   300     grp2_key

Group Name: group3
                  Auth  Acct  DM/  Time
  Server IP Addr  Port  Port  CoA  Window  Encryption Key
  --------------- ----- ----- ---- ------- --------------------------------
  192.168.30.3    1812  1813  No   300     grp3_key
  192.172.40.5    1812  1813  No   300     grp3_key
  192.173.60.7    1812  1813  No   300     grp3_key
```

Figure 4. Example of Output from show server-group radius Command

```
ProCurve(config)# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

             | Login      Server Login      Enable     Server Enable
  Access Task | Primary    Group  Secondary  Primary    Group  Secondary
  ----------- + ---------- ------ ---------- ---------- ------ ----------
  Console     | Local      radius None       Local      radius None
  Telnet      | Local      radius None       Radius     group2 None
  Port-Access | Local             None
  Webui       | Local             None       Local             None
  SSH         | Local             None       Local             None
  Web-Auth    | ChapRadius group3 None
  MAC-Auth    | ChapRadius group3 None
```

Server group information

Figure 5. Example of Output from show authentication Command

```
ProCurve(config)# show accounting

 Status and Counters - Accounting Information

  Interval(min) : 0
  Suppress Empty User : No

  Type     | Method Mode       Server Group
  -------- + ------ ---------- ------------
  Network  | None
  Exec     | Radius Start-Stop group2
  System   | Radius Stop-Only  group2
  Commands | Radius Start-Stop radius
```

Server group information

Figure 6. Example of Output from show accounting Command

- **Enhancement (PR_0000003141)** — Support is added for SSH Secure to RADIUS authentication.

SSH Secure to RADIUS

It is desirable to have an additional method for authentication that allows the storage of passwords in a secure manner rather than as plain text. The MS-CHAPV2 authentication method allows password verification without requiring access to a plain text password. This method is provided for these types of authentication:

- telnet
- SSH
- console

MS-CHAPv2 is currently supported for web authentication and MAC authentication on the switch.

The **aaa authentication** command is modified to provide the MS-CHAPv2 authentication method to the above options. After selecting one of these options, you can choose the authentication method, either **radius** (the default) or the more secure **peap-mschapv2** authentication method.

Syntax: aaa authentication [console | telnet] [enable | login] [radius |peap-mschapv2 | tacacs | local]
aaa authentication web [enable | login] [radius | peap-mschapv2 | local]
aaa authentication ssh [enable | login] [radius | peap-mschapv2 | tacacs | local | public-key]

Select the authentication method, **radius** (*ChapRadius*) *or the more secure* **peap-mschapv2** (*PeapRadius*).

Default: *ChapRadius*

Note An authentication type of “radius” is interpreted as “ChapRadius”.

```
ProCurve(config)# aaa authentication ssh peap-mschapv2
```

Figure 7. Example Command with peap-mschapv2 Option Selected

The show authentication command will display which authentication method has been configured.

```
ProCurve(config)# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

              | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Radius     None       Local      None
  Port-Access | Local      None
  Webui       | Local      None       Local      None
  SSH         | PeapRadius None       Local      None
  Web-Auth    | ChapRadius None
  MAC-Auth    | ChapRadius None
```

Figure 8. Example of show authentication Command Displaying Different Authentication Types

MIB Support

The hpicfAuth.mib will be as follows:

```
hpSwitchAuthenEnablePrimary OBJECT-TYPE
    SYNTAX      INTEGER {
                    local (1),
                    tacacs (2),
                    radius (3),
                    sshPubkey (6),
                    radiusPeapMSChapv2 (7)
                }
```

```
        MAX-ACCESS  read-write
        STATUS      current

        DESCRIPTION  "Indicates the primary authentication mechanism,
                      i.e. whether TACACs+/RADIUS/local will be tried
                      first for a change of a privilege level of session."
    ::= { hpSwitchAuthenEntry 4 }
```

- **Enhancement (PR_0000000083)** — Support is added for a MAC-Auth failure HTTP Redirect option.

MAC-Auth Failure HTTP Redirect Option

Overview. When a client's MAC address is checked by the RADIUS server against the known list of MAC addresses, and the MAC address is not found, the client needs a way to quickly become registered through a web registration process. The HTTP Redirect feature provides a way for a client who has failed MAC authentication to become registered through a web/registration server. Only a web browser is required for this authentication process.

Notes

The HTTP redirect feature cannot be enabled if web authentication is enabled on any port, and conversely, if HTTP redirect is enabled, web authentication cannot be enabled on any port.

The web/registration server software is not included with this feature.

How HTTP Redirect Works. The **unauth-redirect** option must be configured with the registration server's URL as a parameter before HTTP redirect operations can begin. The full URL must be used, for example:

```
http://14.29.16.192:80/myServer.html
or
https://company.com/myServer.html
```

Syntax: [no] aaa port-access mac-based unauth-redirect

Configure the HTTP redirect registration server feature.

<***redirect-URL-str***>

Enable HTTP redirect registration server feature by configuring the URL of the registration page. An entry can have either an IP address or a DNS name. Only one server can be configured.

Note: The entire URL must be used, including the "http://" or "https://" portion.

[restrictive-filter]

Enable the redirect server to only return a Warning or Information page.

[timeout <seconds>]

The time (in seconds) before a client in an unauthorized redirection state is removed from the state tables.

Range: <30-10800> seconds
Default: 1800 seconds

Caution Rogue clients can attempt to access any web pages on the web/registration server via interface ports configured for MAC authentication.

The following steps are involved in HTTP registration.

1. When the redirect feature is enabled, a client that fails MAC authentication is moved into the unauthorized MAC authentication redirection state.
2. A client in the redirect state (having failed MAC authentication) with a web browser open sends a DHCP request. The switch responds with a DHCP lease for an address in the switch's configurable DHCP address range. Additionally, the switch's IP address becomes the client's default gateway. All ARP/DNS requests are handled by the switch and all requests are directed to the switch. The switch replies to these requests with its own address.
3. The client requests a web page. The switch takes this request and responds to the client browser with an HTTP redirect to the configured URL. The client MAC address and interface port are appended as HTTP parameters.
4. Before returning the initial registration page to the client, the switch enables NAT so that all subsequent requests will go to the web server directly. The initial HTML page is returned to the switch and then proxied to the client.
5. After the registration process completes, the registration server updates the RADIUS server with the client's username, password, and profile.
6. The client remains in the redirect state until the client's time exceeds the configured timeout or the switch receives an SNMP deauthentication request from the registration server.
7. The registration server sends an SNMP request to the switch with the MAC identification and interface port to reauthenticate or deauthenticate the client.
8. The switch moves the client out of the special Web/MAC auth redirect state and the client becomes unknown to the switch again. This sets the stage for a new MAC authentication cycle.

Diagram of Registration Process.

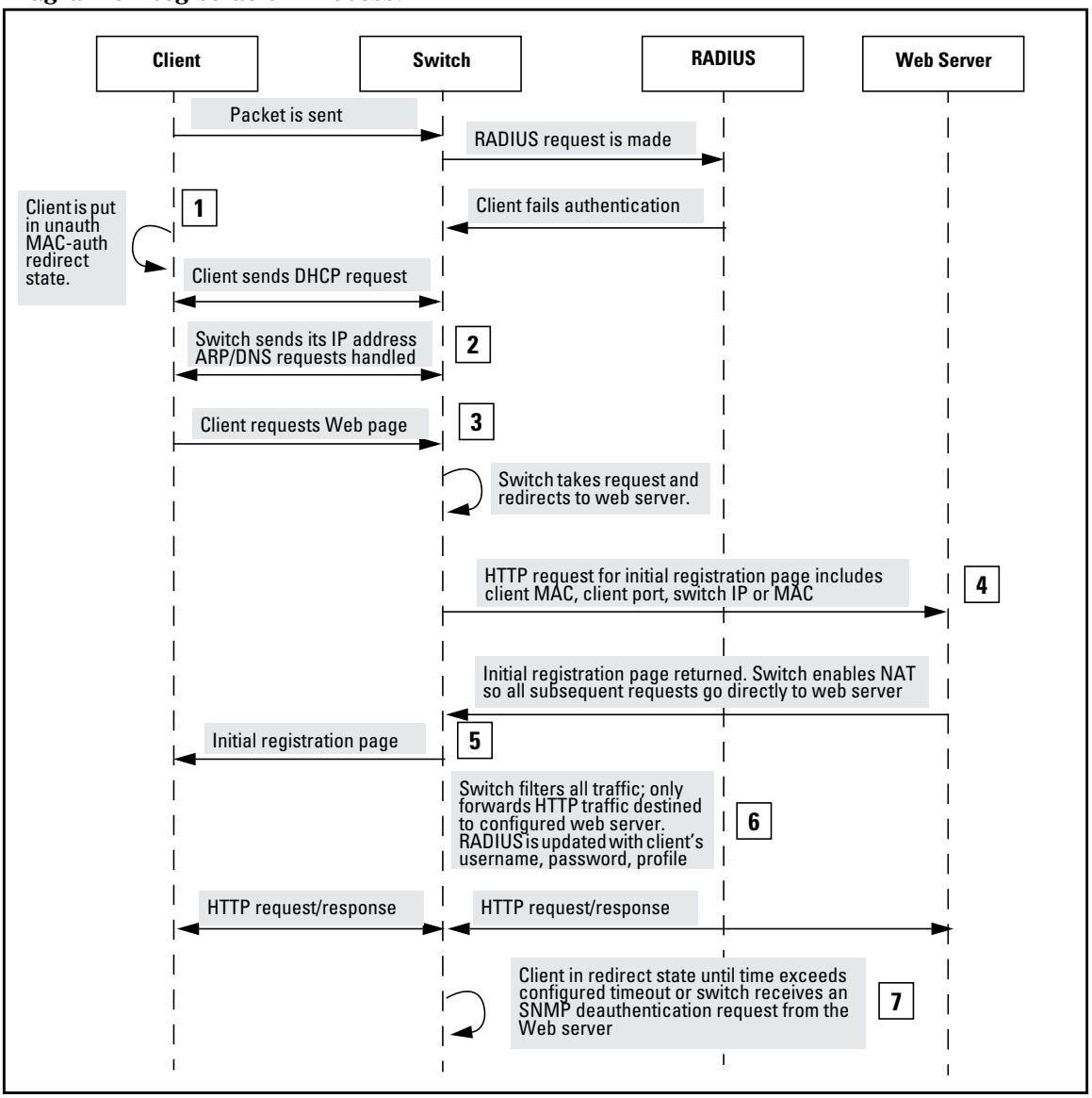


Figure 9. Example of Registration Process Using Redirection

Using the Restrictive-Filter Option. The **restrictive-filter** option allows the switch to reply to all HTTP requests to the switch's IP address with an HTTP-redirect containing the URL of the registration server. It is used when there is no registration process and only a warning or informational page is displayed to the client.

If SSL is not configured, the switch verifies that the MAC address and interface port parameters are present. If SSL is enabled, the switch ensures that the HTTP request is to the registration server's destination IP address.

Show Command Output. Figure 10 is an example of the **show** command that displays the HTTP redirect configuration.

```
ProCurve(config)# show port-access mac-based config

Port Access MAC-Based Configuration

  MAC Address Format : no-delimiter

  Unauth Redirect Configuration URL : http://14.29.16.192:80/myserver.html

  Unauth Redirect Client Timeout (sec) : 1800
  Unauth Redirect Restrictive Filter : Disabled
  Total Unauth Redirect Client Count : 1

                Client Client Logoff    Re-Auth   Unauth   Auth     Cntrl
  Port  Enabled Limit  Moves  Period    Period    VLAN ID  VLAN ID  Dir
  ----- -------- ------ ------ --------- --------- -------- -------- -----
  1     No       1      No     300       0         0        0        both
  2     No       1      No     300       0         0        0        both
  3     No       1      No     300       0         0        0        both
  4     No       1      No     300       0         0        0        both
```

Configured HTTP redirect URL

Figure 10. Example of HTTP Redirect Configuration

Reauthenticating a MAC-Auth Client

Using SNMP. The MIB variable hpicfUsrAuthMacAuthClientReauthenticateEntry in the hpicfUsrAuthMIB provides the capability to reauthenticate a specific MAC-auth client on a port. The MAC address and port are required for SNMP reauthentication.

Using the CLI. To reauthenticate a client using the CLI, use this command:

```
ProCurve(config)# aaa port-access mac-based <single-port>
                  reauthenticate mac-addr <MAC address>
```

The keyword **mac-addr** specifies single client reauthentication. If the **reauthenticate** parameter is entered without the **mac-addr** keyword and MAC address, the command is executed as port reauthentication—all clients on a port are reauthenticated.

Configuring the Registration Server URL. To configure the registration server URL, the command is:

```
ProCurve(config)# aaa port-access mac-based unauth-redirect <URL>
```

For example:

```
ProCurve(config)# aaa port-access mac-based unauth-redirect
                  https://serverA.com:124/registration server/reg.html
```

Unconfiguring a MAC-Auth Registration Server. Each configured registration server's URL must be removed by specifying it exactly, for example:

```
ProCurve(config)# no aaa port-access mac-based unauth-redirect
                  https://serverA.com:124/registration server/reg.html
```

Operating Notes. •If the configured URL contains a domain name (as opposed to an IP address) the switch's DNS resolver must be configured:

- ProCurve(config)# ip dns server-address priority 1 <ipv4-address>

- The NAT does an IP route lookup before it sends the packet to the destination registration server. A VLAN must have been configured that allows the switch to access the registration server.
- The initial page, redirect server, and filter path configuration will be per-switch.

Release K.13.52 Enhancements

Release K.13.52 includes the following enhancements (Not a public release):

- **Enhancement (PR_0000013786)** — Support is added for source IP identification.

Single Source IP Identity

Overview. This enhancement applies to the following software applications:

- TACACS
- RADIUS
- System Logging applications

The above IP-based software applications use a client-server communication model, that is, the client's source IP address is used for unique client identification. The source IP address is determined by the system and is usually the IP address of the outgoing interface in the routing table. However, routing switches may have multiple routing interfaces due to load balancing or routing redundancy, and outgoing packets can potentially be sent by different paths at different times. This results in different source IP addresses, which creates a client identification problem on the server site. For example, there is no way to designate a fixed IP address for outgoing packets for RADIUS or TACACS, so it is necessary to configure in the RADIUS or TACACS database all possible IP addresses that are configured on the switch as valid clients. When using system logging, it can be difficult to interpret the logging and accounting data on the server site as the same client can be logged with different IP addresses.

To decrease the amount of administrative work involved, a configuration model is provided that allows the selection of an IP address to use as the source address for all outgoing traffic generated by a specified software application on the switch. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server.

Specifying the Source IP Address. The CLI command **ip source-interface** is used to specify the source IP address for an application. Different source IP addresses can be used for different software applications, but only one source IP address can be specified for each application. .

Syntax: [no] ip source-interface <radius | tacacs | logging | all> <loopback <***id***> | vlan <***vlan-id***> address <***ip-address***>>

Determines the source IP address used by the specified software application when transmitting IP packets. The **all** *parameter can be used to set one IP address for all the listed applications, in this case, RADIUS, TACACS, and System Logging.*

The **no** *version of the command cancels the configuration and the application reverts to its default behavior. The system determines the source IP address of outgoing application-specific IP packets at packet transmission time.*

loopback <***id***>: *Specifies that the IP address of the loopback interface is used as the source IP address in outgoing packets. If the loopback interface has no IP address, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

vlan <***vlan-id***>: *Specifies that the IP address of the indicated VLAN interface is used as the source IP address of outgoing packets. If the specified VLAN interface has no IP address configured, or is down, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

address <***ip-address***>: *Specifies the IP address that should be used as the source IP address of outgoing packets. The IP address must be a valid IP address configured on one of the switch's VLAN or loopback interfaces. If the interface is down, then the application reverts to the default behavior.*

The Source IP Selection Policy. The source IP address selection for the application protocols is defined through assignment of one of the following policies:

- Outgoing Interface—the IP address of the outgoing IP interface is used as the source IP address. This is the default policy and the default behavior of applications.
- Configured IP Address—the specific IP address that is used as the source IP address. This address is configured on one of the switch's IP interfaces, either a VLAN interface or a Loopback interface.
- Configured IP Interface—the IP address from the specific IP interface (VLAN or Loopback) is used as the source IP address. If there are multiple IP addresses assigned (multinetting, for example), the lowest IP address is used.

If the selection policy cannot be executed because the interface does not have an IP address configured, does not exist, or is down, the application protocol uses the default Outgoing Interface policy. A warning message is displayed, but the configuration changes are accepted. When using the **show ip source-interface status** command to display information about the source IP address selection policy, the administratively-assigned source IP selection policy and the actual (operational) source IP selection policy in effect are displayed. The operational source IP selection policy may be different from the assigned source selection policy if the IP interface does not exist or is down. In this case, the default of Outgoing Interface appears as the operational policy. See Figure 11.

```
ProCurve (config)# show ip source-interface detail

 Source-IP Detailed Information

  Protocol : Tacacs
  Admin Policy           : Configured IP Interface
  Oper Policy            : Outgoing Interface
  Source IP Interface    : Vlan 22
  Source IP Address      : 10.10.10.4
  Source Interface State : Down
```

The Admin Policy differs from the Oper Policy because the Source Interface State is Down. The default Outgoing Interface policy is actually in effect.

Figure 11. Example of the Administratively-assigned Source IP Selection Policy Differing From the Operational Policy

The **no** form of the **ip source-interface** command reverts the application protocols to the default behavior. The Outgoing Interface policy is used.

Figure 12 is an example of assigning a specific source IP address for a RADIUS application. The administrative policy is Configured IP Address.

```
ProCurve(config)# ip source-interface radius address 10.10.10.2

ProCurve(config)# show ip source-interface radius

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Radius   | Configured IP Address   vlan 3         10.10.10.2
```

Figure 12. Example of a Specific IP Address Assigned for the RADIUS Application Protocol

In Figure 13, a VLAN interface (VLAN 22) is specified as the source IP address for TACACS. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface tacacs vlan 22

ProCurve(config)# show ip source-interface tacacs

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Tacacs   | Configured IP Interface vlan 22        10.10.10.4
```

Figure 13. Example of Using a VLAN Interface as the Source IP Address for TACACS

Figure 14 shows a VLAN interface being specified as the source IP address for logging. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface syslog vlan 10

ProCurve(config)# show ip source-interface syslog

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Syslog   | Configured IP Interface vlan 10        10.10.10.10
```

Figure 14. Example of Using a VLAN Interface as the Source IP Address for Logging (Syslog)

Displaying the Source IP Interface Information. There are several **show** commands that can be used to display information about the source IP interface status.

Syntax: show ip source-interface status [radius | tacacs | syslog]

Displays the operational status information for the source IP address selection policy. Both the administratively-assigned source IP selection policy and the operational source IP selection policy are displayed.

When no parameters are specified, policy information for all protocols is displayed.

```
ProCurve(config)# show ip source-interface status

 Source-IP Status Information

  Protocol | Admin Selection Policy  Oper Selection Policy
  -------- + ---------------------- ----------------------
  Tacacs   | Configured IP Interface Configured IP Interface
  Radius   | Configured IP Address   Configured IP Address
  Syslog   | Configured IP Interface Outgoing Interface
```

Figure 15. Example of the Data Displayed for Source IP Interface Status

When executing the **show ip source-interface** command without parameters, the configured IP interfaces (VLANs) and IP addresses are displayed for each protocol.

```
ProCurve(config)# show ip source-interface

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Tacacs   | Configured IP Interface vlan 22        10.10.10.4
  Radius   | Configured IP Address   vlan 3         10.10.10.2
  Syslog   | Configured IP Interface vlan 10        10.10.10.10
```

Figure 16. Example of show ip source-interface Command Output

The **show ip source-interface detail** command displays detailed information about the configured policies, source IP address, and interface state for each protocol.

Syntax: show ip source-interface detail [radius | tacacs | syslog]

Displays detailed operational status information for the source IP address selection policy. Information about the configured policies, source IP address and interface state are displayed.

When no parameters are specified, policy information for all protocols is displayed.

```
ProCurve(config)# show ip source-interface detail

 Source-IP Detailed Information

  Protocol : Tacacs
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : vlan 22
  Source IP Address      : 10.10.10.4
  Source Interface State : Up

  Protocol : Radius
  Admin Policy           : Configured IP Address
  Oper Policy            : Configured IP Address
  Source IP Interface    : vlan 3
  Source IP Address      : 10.10.10.2
  Source Interface State : Up

  Protocol : Syslog
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : vlan 10
  Source IP Address      : 10.10.10.10
  Source Interface State : Up
```

Figure 17. Example of Detailed Information Displayed for Each Protocol

The **show** command can also be used with the application to display the source IP address selection information in effect for the application protocol.

```
ProCurve(config)# show radius

Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :
  Dynamic Authorization UDP Port : 3799
  Source IP Selection : Configured IP address
```

Source IP Selection for the specified application protocol is displayed.

Figure 18. Example of show radius Command Displaying Source IP Selection Information

```
ProCurve(config)# show tacacs

 Status and Counters - TACACS Information

  Timeout : 5
  Source IP Selection : Configured IP Interface
  Encryption Key :
```

Source IP Selection for the specified application protocol is displayed.

Figure 19. Example of show tacacs Command Displaying Source IP Selection Information

```
ProCurve(config)# show debug

Debug Logging

  Source IP Selection: Configured IP interface
  Destination:    None

  Enabled debug types:
   None are enabled.
```

Source IP Selection for the specified application protocol is displayed.

Figure 20. Example of show debug Command Displaying Source IP Selection Information for Syslog

Error Messages. The following error messages may appear when configuring source IP selection if the interface does not exist, is not configured for IP, or is down.

Error Message	Description
Warning: Specified IP address is not configured on any interface	The IP address specified has not been assigned to any interface on the switch.
Warning: Specified IP interface is not configured	The IP interface has not been configured.
Warning: Specified IP interface is not configured for IP	An IP address has not been assigned to this interface.
Warning: Specified IP interface is down.	The interface on the switch associated with this IP address is down.
Warning: Specified IP interface is configured for DHCP	The IP address has not been configured specifically (manually) for this interface and may change.

- **Enhancement (PR_0000008243)** — Support is added for an eavesdrop prevention option.

Optional Eavesdrop Prevention

Overview. Traffic with an unknown destination address is blocked when port security is configured and Eavesdrop Prevention is enabled. Eavesdrop Prevention is enable by default and could not be disabled.

This enhancement provides the ability to disable Eavesdrop Prevention on ports where it may cause problems, such as on ports that are configured to use limited-continuous learning mode.

Feature Interactions. The following table explains the various interactions between learning modes and Eavesdrop Prevention when Eavesdrop Prevention is disabled.

Note When the learning mode is "port-access", Eavesdrop Prevention will not be applied to the port. However, it can still be configured or disabled for the port.

Learn Mode	Effect
Static	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured and only a limited number of static MAC addresses are learned. A device ***must*** generate traffic before the MAC address is learned and traffic is forwarded to it.
Continuous	The default. The Eavesdrop Prevention option does not apply because port security is disabled. Ports forward traffic with unknown destination addresses normally.
Port-access	Disabling Eavesdrop Prevention is not applied to the port. There is no change.
Limited-continuous	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured; MAC addresses age normally. Eavesdrop Prevention may cause difficulties in learning MAC addresses (as with static MAC addresses) and cause serious traffic issues when a MAC ages out.
Configured	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured by a static MAC address. Eavesdrop Prevention should not cause any issues because all valid MAC addresses have been configured.

.

Syntax [no] port-security <***port-list***> eavesdrop-prevention

When this option is enabled, the port is prevented from transmitting packets that have unknown destination addresses. Only devices attached to the port receive packets intended for them. This option does not apply to a learning mode of **port-access** *or* **continuous**.

Default: Enabled

```
ProCurve(config)# show port-security

 Port Security

                            Eavesdrop
  Port  Learn Mode          Prevention  | Action
  ----- ------------------- ----------- + ------------------------
  A1    Continuous          Enabled     | None
  A2    Continuous          Disabled    | None
  A3    Continuous          Enabled     | None
  A4    Continuous          Disabled    | None
  A5    Continuous          Enabled     | None
  A6    Continuous          Enabled     | None
  A7    Continuous          Disabled    | None
  A8    Continuous          Disabled    | None
  A9    Continuous          Enabled     | None
```

Figure 21. Example of show port-security Command Displaying Eavesdrop Prevention

MIB Support. The following MIB support is provided for Eavesdrop Prevention.

```
hpSecPtPreventEavesdrop OBJECT-TYPE
  SYNTAX        INTEGER {
                  enable (1),
                  disable (2)
                }
MAX-ACCESS read-write
STATUS   current
DESCRIPTION
      "If enabled on a switch, outbound unknown unicast
       packets will not be forwarded out this port. If
       enabled on a repeater, outbound unknown unicast
       packets for this port will be scrambled.
::= { hpSecurePortEntry 5 }
```

Release K.14.03 Enhancements

The following enhancements, present in K.13.40 and newer K.13 versions, are NOT present in K.14.03:

- **Enhancement (PR_0000003127)** — Link Trap and LACP Global Enable/Disable.
- **Enhancement (PR_0000003128)** — The ability to clear statistics was added.
- **Enhancement (PR_0000003718)** — The MAC Lockout limit was increased to 64.
- **Enhancement (PR_0000007388)** — The ability to configure logging via SNMP was added.
- The following enhancement, present in K.13.43 and newer K.13 versions, is NOT present in K.14.03:
- **Enhancement (PR_0000003557)** — The ability to enable/disable the USB port via CLI and SNMP was added.

The following enhancements, present in K.13.51 and newer K.13 versions, are NOT present in K.14.03.

- **Enhancement (PR_0000003144)** — Support was added for multiple RADIUS groups.
- **Enhancement (PR_0000003141)** — Support was added for SSH Secure to RADIUS authentication.
- **Enhancement (PR_0000000083)** — Support was added for a MAC-Auth failure HTTP Redirect option.

The following enhancements, present in K.13.52 and newer K.13 versions, are NOT present in K.14.03.

- **Enhancement (PR_0000013786)** — Support was added for source IP identification.
- **Enhancement (PR_0000008243)** — Support was added for an eavesdrop prevention option.

Release K.14.04 through K.14.08 Enhancements

No new enhancements, software never built.

Release K.14.09 Enhancements

Release K.14.09 includes the following enhancements.

- **Enhancement (0000017065)** — Support was added for the HP ProCurve 6600 Switch Premium License (J9305A) features.

Release K.14.09 is a major software update containing many new features and enhancements to existing features.

Software Manual/ Enhancements	Description
Management and Configuration Guide	
Advanced Classifier-Based Mirroring:	More flexible and powerful port- and VLAN-based mirroring, including a finer granularity for selecting the inbound IP traffic that you want to mirror. See also "Classifier-Based Software Configuration" in the ***Advanced Traffic Management Guide***.
Global Mirroring Updates:	Deprecation and automatic conversion of ACL-based mirroring to classifier-based mirroring configuration in release K.14.xx. Support for **no-tag-added** option in direction-based mirroring on port interfaces, which allows you to exclude the VLAN tag added to packets sent as mirrored copies of selected traffic to a mirroring destination.
Distributed Trunking:	Allows a server to connect to multiple switches with a single logical trunk enabling load-balancing and redundancy.
Debug, Syslog, and Show Command Updates:	New enhancements include: • Enhanced diagnostics and debug information on features such as IP routing, LLDP, OSPF, SSH, VRRP and Wireless Services. • The **logging facility** command enables you to specify the destination subsystem used in a configured Syslog server. • Pattern matching option with the **show** command provides the ability to do searches for specific text. Selected portions of the output are displayed, depending on the parameters chosen. See the ***Troubleshooting*** appendix for details.
ACE Hit Counts:	ACE matches (hits) for permit and deny entries can be tracked using the **show statistics** < aclv4 | aclv6 > command. See the ***Troubleshooting*** appendix for details.
Ping/Traceroute Updates:	The Ping, Ping6, Traceroute and Traceroute6 commands now include a **source** < ***ip-addr*** | ***vid*** > option. See the ***Troubleshooting*** appendix for details.
Core-Dump File Capture:	Allows for the automatic generation of core-dump files for enhanced debugging capabilities in the event of system failure.
Advanced Traffic Management Guide	

Software Manual/ Enhancements	Description
Classifier-Based Configuration:	Classifier-based service policies are designed to work with existing globally-configured, switch-wide and port-wide configurations by allowing you to zoom in on a subset of port or VLAN traffic. Using multiple match criteria, you can finely select and define the classes of traffic that you want to manage. Policy actions determine how you can handle the selected traffic. See also "Advanced Classifier-Based Mirroring" in the ***Management and Configuration Guide*** and "Advanced Classifier-Based QoS" in the ***Advanced Traffic Management Guide***.
Advanced Classifier-Based QoS:	More flexible and powerful QoS classification and enforcement, including: • A finer granularity for classifying inbound IPv4 and IPv6 traffic • Additional actions for managing selected traffic, such as rate-limiting and IP precedence marking See also ***Classifier-Based Software Configuration***.
Global QoS enhancements:	Support for IPv6 addresses, IPv6 prefixes, and IPv4 subnet masks in global QoS configuration and "show" commands has been added. See also ***DSCP Mapping Updates***.
DSCP Mapping Updates:	Support for additional DSCP codepoint values in global and classifier-based QoS commands that remark packets and remap DSCP-802.1p priority assignments.
Management VLAN:	The Management VLAN feature applies to both IPv4 and IPv6 traffic.
Routing and Multicast Guide	
ECMP Routing for Static Routes:	Supports optional load-sharing across redundant links by allowing OSPF to add two, three, or four equal-cost next-hop routes for traffic to different subnets.
OSPF Display Commands:	Enhanced **show ip ospf statistics**, **clear ip ospf statistics**, and **show ip ospf spf-log** commands. See also updates to the **debug ip ospf** command in the ***Troubleshooting*** appendix in the ***Management and Configuration Guide.***
Access and Security Guide	
Management Interface Wizard:	Allows easy configuration of secure management interfaces at initial setup using either the CLI or Web browser interface.
RADIUS COS Updates:	802.1p (CoS) Priority for traffic inbound to the switch has changed from per-port to per-user.
RADIUS Rate-Limiting Updates:	Includes: • traffic inbound (ingress) to the switch has changed from per-port to per-user • traffic per-port outbound (Egress) from the switch has been added
RADIUS ACLs:	Enhanced support for dynamic (RADIUS-assigned) ACLs capable of filtering both IPv4 and IPv6 traffic from authenticated clients.
IP SSH for IPv4 and IPv6:	SSH is now automatically supported for both IPv4 and IPv6 when SSH is enabled. The **ip-version < 4 | 6 | 4or6 >** command has been removed.
Ipv6 Configuration Guide	
IPv6 ACLs:	Support has been added for static IPv6 ACLs per-VLAN and per-port.
[no] telnet6-server [DEPRECATED]:	The **[no] telnet6-server** command has been replaced by the **[no] telnet-server** command, which formerly was used only for IPv4 Telnet. The **telnet-server** command now enables or disables both IPv4 and IPv6 Telnet.
clear ipv6 neighbors	No longer lists removed addresses. Neighbor entries for active routers are not removed, but their layer-2 information is cleared.

Note on Manual Updates:

With this release, the new 6600 platform has been added to the 3500yl/5400zl/6200yl/8200zl manual set. As before, where features apply only to a specific model or models, this will be indicated in the chapter or heading for that feature; for example, "Redundancy (Switch 8212zl)" or "Stack Management for the Series 3500yl Switches and the 6200yl Switch."

Release K.14.10 Enhancements

Release K.14.10 includes the following enhancements.

- **Enhancement (PR_0000011224)** — Support was added for chassis locator LED status with the CLI.

Locator LED Status via CLI

The **chassislocate** parameter provides a way to check the status of the blue Locator LED with a CLI command. The status will be displayed, and if the status is ON or BLINK, the amount of time the LED will continue to be on or to blink is displayed.

Syntax: show system chassislocate

Displays the chassis Locator LED status. Possible values are On, Off, or Blink. When the status is On or Blink, the number of minutes that the Locator LED will continue to be on or to blink is displayed.

```
ProCurve(config)# show system chassislocate

Chassis Locator LED: ON 5 minutes 5 seconds

ProCurve(config)# show system chassislocate

Chassis Locator LED: BLINK 10 minutes 6 seconds

ProCurve(config)# show system chassislocate

Chassis Locator LED: OFF
```

Figure 22. Example of Command Results for show system chassislocate Command

- **Enhancement (PR_0000011601)** — Support was added for an increased number of LACP trunk groups.

Increase in Number of Trunk Groups

The number of trunk groups per switch is increased from 60 trunk groups to 144 trunk groups. The maximum number of ports per trunk remains at eight. The trunks do not have to be the same size, for example 100 two-port trunks and 11 eight-port trunks are supported.

- **Enhancement (PR_0000010201)** — Support was added for SNTP client authentication.

SNTP—Client Authentication

Overview. Enabling SNTP authentication allows network devices such as HP switches to validate the SNTP messages received from an NTP or SNTP server before updating the network time. NTP or SNTP servers and clients must be configured with the same set of authentication keys so that the servers can authenticate the messages they send and clients (HP switches) can validate the received messages before updating the time.

This enhancement provides support for SNTP client authentication on HP switches, which addresses security considerations when deploying SNTP in a network.

For more information about SNTP operation in general, see the chapter “Time Protocols” in the *Management and Configuration Guide* for your switch.

Requirements

The following must be configured to enable SNTP client authentication on the switch.

SNTP Client Authentication Support. ■Timesync mode must be SNTP. Use the **timesync sntp** command. (SNTP is disabled by default.)

- SNTP must be in unicast or broadcast mode. See "Configuring Unicast and Broadcast Mode" on page 65.
- The MD5 authentication mode must be selected.
- An SNTP authentication key-identifier (**key-id**) must be configured on the switch and a value (**key-value**) must be provided for the authentication key. A maximum of 8 sets of **key-id** and **key-value** can be configured on the switch.
- Among the keys that have been configured, one key or a set of keys must be configured as trusted. Only trusted keys will be used for SNTP authentication.
- If the SNTP server requires authentication, one of the trusted keys has to be associated with the SNTP server.
- SNTP client authentication must be enabled on the ProCurve switch. If client authentication is disabled, packets are processed without authentication. All of the above steps are necessary to enable authentication on the client.

Note **SNTP Server Authentication Support**. SNTP server is not supported on ProCurve products.

The following must be performed on the SNTP server:

- The same authentication key-identifier, trusted key, authentication mode and key-value that were configured on the SNTP client must also be configured on the SNTP server.
- SNTP server authentication must be enabled on the server.

If any of the parameters on the server are changed, the parameters have to be changed on all the SNTP clients in the network as well. The authentication check will fail on the clients otherwise, and the SNTP packets will be dropped.

Configuring the Key-Identifier, Authentication Mode, and Key Value. This command configures the **key-id**, **authentication-mode**, and **key-value**, which are required for authentication. It is executed in the global configuration context.

Syntax: sntp authentication key-id <***key-id***> authentication-mode <md5> key-value <***key-string***> [trusted]
no sntp authentication key-id <***key-id***>

Configures a key-id, authentication-mode (MD5 only), and key-value, which are required for authentication.

The **no** *version of the command deletes the authentication key.*

Default: No default keys are configured on the switch.

key-id: *A numeric key identifier in the range of 1-4,294,967,295 (2^{32})that identifies the unique key value. It is sent in the SNTP packet.*

key-value <*key-string*>: *The secret key that is used to generate the message digest. Up to 32 characters are allowed for <**key-string**>.*

```
ProCurve(config)# sntp authentication key-id 55 authentication-mode md5 key-
value secretkey1
```

Figure 23. Example of Setting Parameters for SNTP Authentication

Configuring a Trusted Key. Trusted keys are used in SNTP authentication. In unicast mode, a **trusted** key must be associated with a specific NTP/SNTP server. That key is used for authenticating the SNTP packet.

In unicast mode, a specific server is configured on the switch so that the SNTP client communicates with the specified server to get the date and time.

In broadcast mode, the SNTP client switch checks the size of the received packet to determine if it is authenticated. If the broadcast packet is authenticated, the key-id value is checked to see if the same key-id value is configured on the SNTP client switch. If the switch is configured with the same key-id value and the key-id value is configured as "trusted", the authentication succeeds. Only trusted key-id value information is used for SNTP authentication. See"Configuring Unicast and Broadcast Mode" on page 65 for information about configuring these modes.

If the packet contains key-id value information that is not configured on the SNTP client switch or the received packet contains no authentication information, it is discarded. The SNTP client switch expects packets to be authenticated if SNTP authentication is enabled.

When authentication succeeds, the time in the packet is used to update the time on the switch.

Enter the following command to configure a **key-id** as **trusted**.

Syntax: sntp authentication key-id <***key-id***> trusted
no sntp authentication key-id <***key-id***> trusted

Trusted keys are used during the authentication process. The switch can be configured with up to eight sets of key-id/key-value pairs. One specific set must selected for authentication; this is done by configuring the set as **trusted**.

The **key-id** *itself must already be configured on the switch. To enable authentication, at least one* **key-id** *must be configured as* **trusted**.

The **no** *version of the command indicates the key is unreliable (not trusted).*

Default: No key is trusted by default.

Associating a Key with an SNTP Server. After a key is configured, it must be associated with a specific server.

Syntax: [no] sntp server priority <1-3> <ip-address | ipv6-address> <***version-num***> [key-id <***1-4,294,967,295***>]

Configures a **key-id** *to be associated with a specific server. The key itself must already be configured on the switch.*

The **no** *version of the command disassociates the key from the server. This does not remove the authentication key.*

Default: No key is associated with any server by default.

priority*: Specifies the order in which the configured servers are polled for getting the time. Value is between 1 and 3.*

<version-num> *Specifies the SNTP software version to use, and is assigned on a per-server basis. The version setting is backwards-compatible. For example, using version 3 means that the switch accepts versions 1 through 3.*

Default: 3; range: 1 - 7.

key-id: *Optional command. The key identifier (range 1-4,294,967,295) sent in the SNTP packet. This* **key-id** *will be associated with the SNTP server specified in the command.*

```
ProCurve(config)# sntp server priority 1 10.10.19.5 2 key-id 55
```

Figure 24. Example of Associating a Key-Id with a Specific Server

Enabling SNTP Client Authentication. The **sntp authentication** command enables SNTP client authentication on the switch. If SNTP authentication is not enabled, SNTP packets are not authenticated.

Syntax: [no] sntp authentication

Enables the SNTP client authentication

The **no** *version of the command disables authentication.*

Default: SNTP client authentication is disabled by default.

Configuring Unicast and Broadcast Mode. To enable authentication, either unicast or broadcast mode must be configured. When authentication is enabled, changing the mode from unicast to broadcast or vice versa is not allowed. You must disable authentication and then change the mode.

To set the SNTP mode or change from one mode to the other, enter the appropriate command.

Syntax: sntp unicast
sntp broadcast

Enables SNTP for either broadcast or unicast mode.

Default: SNTP mode is disabled by default. SNTP does not operate even if specified by the CLI **timesync** *command or by the menu interface* **Time Sync Method** *parameter.*

Unicast: *Directs the switch to poll a specific server periodically for SNTP time synchronization. The default value between each polling request is 720 seconds but can be configured. At least one manually configured server IP address is required.*

Note: At least one **key-id** *must be configured as* **trusted** *and it must be associated with one of the SNTP servers. To edit or remove the associated* **key-id** *information or SNTP server information. SNTP authentication must be disabled.*

Broadcast: *Directs the switch to acquire its time synchronization from data broadcast by any SNTP server to the network broadcast address. The switch uses the first server detected and ignores any others. However, if the Poll Interval (configurable up to 720 seconds) expires three times without the switch detecting a time update from the original server, the switch accepts a broadcast time update from the next server it detects.*

Displaying SNTP Configuration Information. The **show sntp** command displays SNTP configuration information, including any SNTP authentication keys that have been configured on the switch.

```
ProCurve(config)# show sntp

 SNTP Configuration

  SNTP Authentication : Enabled
  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 720


  Priority SNTP Server Address                    Protocol Version KeyId
  -------- ---------------------------------------  ---------------- -----
  1        10.10.10.2                             3                55
  2        fe80::200:24ff:fec8:4ca8               3                55
```

Figure 25. Example of SNTP Configuration Information

To display all the SNTP authentication keys that have been configured on the switch, enter the **show sntp authentication** command.

```
ProCurve(config)# show sntp authentication

  SNTP Authentication Information

  SNTP Authentication : Enabled

  Key-ID  Auth Mode  Trusted
  ------- ---------- --------
  55      MD5        Yes
  10      MD5        No
```

Figure 26. Example of show sntp authentication Command Output

To display the statistical information for each SNTP server, enter the **sntp statistics** command. The number of SNTP packets that have failed authentication is displayed for each SNTP server address.

```
ProCurve(config)# show sntp statistics
SNTP Statistics

  Received Packets  : 0
  Sent Packets      : 3
  Dropped Packets   : 0

  SNTP Server Address                          Auth Failed Pkts
  -------------------------------------        ----------------
  10.10.10.1                                       0
  fe80::200:24ff:fec8:4ca8                         0
```

Figure 27. Example of SNTP Authentication Statistical Information

Saving Configuration Files and the Include-Credentials Command. You can use the **include-credentials** command to store security information in the running-config file. This allows you to upload the file to a TFTP server and then later download the file to the ProCurve switches on which you want to use the same settings. For more information about the **include-credentials** command, see "Configuring Username and Password Security" in the *Access Security Guide* for your switch.

The authentication key values are shown in the output of the **show running-config** and **show config** commands only if the **include-credentials** command was executed.

When SNTP authentication is configured and **include-credentials** has not been executed, the SNTP authentication configuration is not saved.

```
ProCurve(config)# show config

Startup configuration:

.
.
.
timesync sntp
sntp broadcast
sntp 50
sntp authentication
sntp server priority 1 10.10.10.2 3 key-id 55
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4 key-id 55
.
.
.
```

SNTP authentication has been enabled and a key-id of 55 has been created.

Figure 28. Example of Configuration File with SNTP Authentication Information

In Figure 28, the **include-credentials** command has not been executed and is not present in the configuration file. The configuration file is subsequently saved to a TFTP server for later use. The SNTP authentication information is not saved and is not present in the retrieved configuration file, as shown in Figure 29.

```
ProCurve(config)#copy tftp startup-config 10.2.3.44 config1

.
.
.
Switch reboots...

Startup configuration
.
.
.
timesync sntp
sntp broadcast
sntp 50 sntp server priority 1 10.10.10.2 3
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4
.
.
.
```

The **sntp authentication** line and the **key-id**s are not displayed. You must reconfigure SNTP authentication.

Figure 29. Example of a Retrieved Configuration File When Include Credentials is not Configured

If **include-credentials** is configured, the SNTP authentication configuration is saved in the configuration file. When the **show config** command is entered, all of the information that has been configured for SNTP authentication displays, including the key-values.

```
ProCurve(config)# show config

Startup configuration:

.                          Include-credentials is configured.
.
.
include-credentials
timesync sntp                                  All of the SNTP authentication
sntp broadcast                                 information displays in the
sntp 50                                        configuration file, including the key-
sntp authentication                            values.
sntp authentication key-id 55 authentication-mode md5 key-value “secretkey1”
trusted
sntp authentication key-id 2 authentication-mode md5 key-value “secretkey2”
sntp server priority 1 10.10.10.2 3 key-id 55
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4 key-id 55
sntp server priority 3 10.10.4.60 3
.
.
.
```

Figure 30. Example of Saved SNTP Authentication Information when include-credentials is Configured

- **Enhancement (PR_0000013247)** — Support was added for the **show VLANs custom** CLI commands.

Show VLANs Custom

The **show vlans custom** command allows you to customize the information displayed when executing the **show vlans** command.

Syntax: show vlans custom [port <***port-list***>] column-list

Select the information that you want to display in the order you want to display it for the **show vlans** *command. You can display information for one port or range of ports. If <port-list> isn't specified, then all ports display.*

Fields that can be included in the customized display are shown in the table below.

Field	Display	Example	Default
id	VLAN Id	5	6
name	VLAN Name	Vlan55	32
status	Status	Port-based	10
voice	Voice enabled	No	5
jumbo	Jumbos enabled	No	5
ipconfig	How the ip address was configured	Manual Disabled DHCP/BootP	10
ipaddr (IPv4) ipaddr (IPv6)	the IP address(es)	10.10.10.3 fe80::212:79ff:fe8d:8000	15 for IPv4 46 for IPv6
ipmask	The subnet mask(s)	255.255.255.6 /64 (prefix for IPv6 is in format “/XX”)	15
proxyarp	Whether proxy arp is configured	No	5
localproxyarp	Whether local proxy arp is configured	No	9
state	“Up” if at least one port is up	Up	5

The example in Figure 31 displays **id** at its default width, and will show up to 20 characters of the VLAN **name**. The columns selected for display are separated by spaces.

```
ProCurve(config)# show vlan custom A1-A3 id name:20 ipaddr state

Status and Counters - VLAN Information - Custom view

 VLANID VLAN name             IP Addr                          State
 ------ --------------------  -------------------------------- -----
 1      DEFAULT_VLAN          15.255.134.74                    Up
 33     Vlan33                10.10.10.01                      Up
 44     Vlan44                15.255.164.13                    Up
 55     Vlan55                15.255.178.2                     Down
                              15.255.178.3
                              15.255.178.4
 60     Vlan60                fe80::212:79ff:fe8d:8000%vlan60  Up
```

Figure 31. Example of show vlan custom Command

If the width of the column requested is smaller than the header name of the column, the display of the header name is truncated.

```
ProCurve(config)# show vlan custom id
Status and Counters - VLAN Information - Custom view

 VLANID
 ------
 1
 33
 44

ProCurve(config)# show vlan custom id:2
Status and Counters - VLAN Information - Custom view

 VL
 --
 1
 33
 44
```

Figure 32. Example of Column Headers

The total output will wrap if it is longer than the terminal width (for example, 80 characters). It is not truncated.

Creating an Alias for Show VLAN Commands

You can create an alias for a frequently used **show vlans custom** command to avoid entering the selected columns each time you use the command.

```
ProCurve(config)# alias showvlanstatus = “show vlan custom A1-A3 id name:20
status”

ProCurve(config)# showvlanstatus
Status and Counters - VLAN Information - Custom view

 VLANID VLAN name            Status
 ------ -------------------- ----------
 1      DEFAULT_VLAN         Port-based
 33     Vlan33               Port-based
```

Figure 33. Example of the alias Command

Note on Using Pattern Matching with the “Show VLANs Custom” Command

If you have included a pattern matching command to search for a field in the output of the **show vlan custom** command and the **show vlans custom** command produces an error, the error message may not be visible and the output is empty. For example, if you enter a command that produces an error (vlan is misspelled) with the pattern matching **include** option:

```
ProCurve(config)# show vlans custom 1-3 name vlun | include vlan1
```

the output may be empty. It is advisable to try the **show vlans custom** command first to ensure there is output, and then enter the command again with the pattern matching option.

Release K.14.24 Enhancements

- **Enhancement (PR_0000041097)** — Support is added for the HP ProCurve 6600-48G (J9451A) and HP ProCurve 6600-48G-4XG (J9452A) Switches.

Release K.14.31 Enhancements

- **Enhancement (PR_0000013786)** — Support is added for source IP identification. For more information, see “Release K.13.52 Enhancements” on page 53“.

Single Source IP Identity

Overview. This enhancement applies to the following software applications:

- TACACS
- RADIUS
- System Logging applications

The above IP-based software applications use a client-server communication model, that is, the client’s source IP address is used for unique client identification. The source IP address is determined by the system and is usually the IP address of the outgoing interface in the routing table. However, routing switches may have multiple routing interfaces due to load balancing or routing redundancy, and outgoing packets can potentially be sent by different paths at different times. This results in different source IP addresses, which creates a client identification problem on the server site. For example, there is no way to designate a fixed IP address for outgoing packets for RADIUS or TACACS, so it is necessary to configure in the RADIUS

or TACACS database all possible IP addresses that are configured on the switch as valid clients. When using system logging, it can be difficult to interpret the logging and accounting data on the server site as the same client can be logged with different IP addresses.

To decrease the amount of administrative work involved, a configuration model is provided that allows the selection of an IP address to use as the source address for all outgoing traffic generated by a specified software application on the switch. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server.

Specifying the Source IP Address. The CLI command **ip source-interface** is used to specify the source IP address for an application. Different source IP addresses can be used for different software applications, but only one source IP address can be specified for each application.

Syntax: [no] ip source-interface <radius | tacacs | logging | all> <loopback <***id***> | vlan <***vlan-id***> address <***ip-address***>>

Determines the source IP address used by the specified software application when transmitting IP packets. The **all** *parameter can be used to set one IP address for all the listed applications, in this case, RADIUS, TACACS, and System Logging.*

The **no** *version of the command cancels the configuration and the application reverts to its default behavior. The system determines the source IP address of outgoing application-specific IP packets at packet transmission time.*

loopback <***id***>: *Specifies that the IP address of the loopback interface is used as the source IP address in outgoing packets. If the loopback interface has no IP address, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

vlan <***vlan-id***>: *Specifies that the IP address of the indicated VLAN interface is used as the source IP address of outgoing packets. If the specified VLAN interface has no IP address configured, or is down, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

address <***ip-address***>: *Specifies the IP address that should be used as the source IP address of outgoing packets. The IP address must be a valid IP address configured on one of the switch's VLAN or loopback interfaces. If the interface is down, then the application reverts to the default behavior.*

The Source IP Selection Policy. The source IP address selection for the application protocols is defined through assignment of one of the following policies:

- Outgoing Interface—the IP address of the outgoing IP interface is used as the source IP address. This is the default policy and the default behavior of applications.
- Configured IP Address—the specific IP address that is used as the source IP address. This address is configured on one of the switch's IP interfaces, either a VLAN interface or a Loopback interface.
- Configured IP Interface—the IP address from the specific IP interface (VLAN or Loopback) is used as the source IP address. If there are multiple IP addresses assigned (multinetting, for example), the lowest IP address is used.

If the selection policy cannot be executed because the interface does not have an IP address configured, does not exist, or is down, the application protocol uses the default Outgoing Interface policy. A warning message is displayed, but the configuration changes are accepted. When using the **show ip source-interface status** command to display information about the source IP address selection policy, the administratively-assigned source IP selection policy and the actual (operational) source IP selection policy in effect are displayed. The operational source IP selection policy may be different from the assigned source selection policy if the IP interface does not exist or is down. In this case, the default of Outgoing Interface appears as the operational policy. See Figure 34.

```
ProCurve (config)# show ip source-interface detail

 Source-IP Detailed Information

  Protocol : Tacacs
  Admin Policy           : Configured IP Interface
  Oper Policy            : Outgoing Interface
  Source IP Interface    : Vlan 22
  Source IP Address      : 10.10.10.4
  Source Interface State : Down
```

The Admin Policy differs from the Oper Policy because the Source Interface State is Down. The default Outgoing Interface policy is actually in effect.

Figure 34. Example of the Administratively-assigned Source IP Selection Policy Differing From the Operational Policy

The **no** form of the **ip source-interface** command reverts the application protocols to the default behavior. The Outgoing Interface policy is used.

Figure 12 is an example of assigning a specific source IP address for a RADIUS application. The administrative policy is Configured IP Address.

```
 ProCurve(config)# ip source-interface radius address 10.10.10.2

 ProCurve(config)# show ip source-interface radius

  Source-IP Configuration Information

   Protocol | Admin Selection Policy  IP Interface   IP Address
   -------- + ---------------------- -------------- ---------------
   Radius   | Configured IP Address   vlan 3         10.10.10.2
```

Figure 35. Example of a Specific IP Address Assigned for the RADIUS Application Protocol

In Figure 13, a VLAN interface (VLAN 22) is specified as the source IP address for TACACS. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface tacacs vlan 22

ProCurve(config)# show ip source-interface tacacs

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Tacacs   | Configured IP Interface vlan 22        10.10.10.4
```

Figure 36. Example of Using a VLAN Interface as the Source IP Address for TACACS

Figure 14 shows a VLAN interface being specified as the source IP address for logging. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface syslog vlan 10

ProCurve(config)# show ip source-interface syslog

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Syslog   | Configured IP Interface vlan 10        10.10.10.10
```

Figure 37. Example of Using a VLAN Interface as the Source IP Address for Logging (Syslog)

Displaying the Source IP Interface Information. There are several **show** commands that can be used to display information about the source IP interface status.

Syntax: show ip source-interface status [radius | tacacs | syslog]

Displays the operational status information for the source IP address selection policy. Both the administratively-assigned source IP selection policy and the operational source IP selection policy are displayed.

When no parameters are specified, policy information for all protocols is displayed.

```
ProCurve(config)# show ip source-interface status

 Source-IP Status Information

  Protocol | Admin Selection Policy  Oper Selection Policy
  -------- + ---------------------- ----------------------
  Tacacs   | Configured IP Interface Configured IP Interface
  Radius   | Configured IP Address   Configured IP Address
  Syslog   | Configured IP Interface Outgoing Interface
```

Figure 38. Example of the Data Displayed for Source IP Interface Status

When executing the **show ip source-interface** command without parameters, the configured IP interfaces (VLANs) and IP addresses are displayed for each protocol.

```
 ProCurve(config)# show ip source-interface

  Source-IP Configuration Information

   Protocol | Admin Selection Policy  IP Interface   IP Address
   -------- + ---------------------- -------------- ---------------
   Tacacs   | Configured IP Interface vlan 22        10.10.10.4
   Radius   | Configured IP Address   vlan 3         10.10.10.2
   Syslog   | Configured IP Interface vlan 10        10.10.10.10
```

Figure 39. Example of show ip source-interface Command Output

The **show ip source-interface detail** command displays detailed information about the configured policies, source IP address, and interface state for each protocol.

Syntax: show ip source-interface detail [radius | tacacs | syslog]

Displays detailed operational status information for the source IP address selection policy. Information about the configured policies, source IP address and interface state are displayed.

When no parameters are specified, policy information for all protocols is displayed.

```
ProCurve(config)# show ip source-interface detail

 Source-IP Detailed Information

  Protocol : Tacacs
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : vlan 22
  Source IP Address      : 10.10.10.4
  Source Interface State : Up

  Protocol : Radius
  Admin Policy           : Configured IP Address
  Oper Policy            : Configured IP Address
  Source IP Interface    : vlan 3
  Source IP Address      : 10.10.10.2
  Source Interface State : Up

  Protocol : Syslog
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : vlan 10
  Source IP Address      : 10.10.10.10
  Source Interface State : Up
```

Figure 40. Example of Detailed Information Displayed for Each Protocol

The **show** command can also be used with the application to display the source IP address selection information in effect for the application protocol.

```
ProCurve(config)# show radius

Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :
  Dynamic Authorization UDP Port : 3799
  Source IP Selection : Configured IP address   <-- Source IP Selection for the specified application protocol is displayed.
```

Figure 41. Example of show radius Command Displaying Source IP Selection Information

```
ProCurve(config)# show tacacs

 Status and Counters - TACACS Information

  Timeout : 5
  Source IP Selection : Configured IP Interface
  Encryption Key :
```

Source IP Selection for the specified application protocol is displayed.

Figure 42. Example of show tacacs Command Displaying Source IP Selection Information

```
ProCurve(config)# show debug

Debug Logging

  Source IP Selection: Configured IP interface
  Destination:    None

  Enabled debug types:
   None are enabled.
```

Source IP Selection for the specified application protocol is displayed.

Figure 43. Example of show debug Command Displaying Source IP Selection Information for Syslog

Error Messages. The following error messages may appear when configuring source IP selection if the interface does not exist, is not configured for IP, or is down.

Error Message	Description
Warning: Specified IP address is not configured on any interface	The IP address specified has not been assigned to any interface on the switch.
Warning: Specified IP interface is not configured	The IP interface has not been configured.
Warning: Specified IP interface is not configured for IP	An IP address has not been assigned to this interface.
Warning: Specified IP interface is down.	The interface on the switch associated with this IP address is down.
Warning: Specified IP interface is configured for DHCP	The IP address has not been configured specifically (manually) for this interface and may change.

- **Enhancement (PR_0000003718)** — The MAC Lockout limit was increased. For more information, see “Release K.13.40 Enhancements” on page 40.
- **Enhancement (PR_0000003127)** — Link Trap and LACP Global Enable/Disable. For more information, see “Release K.13.40 Enhancements” on page 40.
- **Enhancement (PR_0000003128)** — The ability to clear statistics was added. For more information, see “Release K.13.40 Enhancements” on page 40.
- **Enhancement (PR_0000016121)** — Support is added for multiple RADIUS groups. For more information, see “Release K.13.51 Enhancements” on page 44.
- **Enhancement (PR_0000003141)** — Support is added for SSH Secure to RADIUS authentication. For more information, see “Release K.13.51 Enhancements” on page 44.

- **Enhancement (PR_0000000083)** — Support is added for a MAC-Auth failure HTTP Redirect option. For more information, see "Release K.13.51 Enhancements" on page 44.
- **Enhancement (PR_0000008243)** — Support is added for an eavesdrop prevention option.For more information, see"Release K.13.52 Enhancements" on page 53.
- **Enhancement (PR_0000013992)** — The ability to disable 5V power to the USB port is added.

USB Port Config via CLI and SNMP

CLI Implementation. This feature allows configuration of the USB port with either the CLI or SNMP.

To enable/disable the USB port with the CLI:

Syntax: usb-port
no usb-port

Enables the USB port. The **no** *form of the command disables the USB port and any access to the device.*

To display the status of the USB port:

Syntax: show usb-port

Displays the status of the USB port. It can be enabled, disabled, or not present.

```
ProCurve(config)# show usb-port

  USB port status: enabled
  USB port power status: power on      (USB device detected in port)
  USB port reseat status: USB reseat not required
```

Figure 44. Example of show usb-port Command Output on version K.13.59 and later

```
ProCurve(config)# show usb-port

  USB port status: enabled
  USB port power status: power on    (USB device detected in port)
```

Figure 45. Example of show usb-port Command Output on version K.14.XX

One of the following messages indicates the presence or absence of the USB device:

- `Not able to sense device in USB port`
- `USB device detected in port`
- `no USB device detected in port`

The reseat status messages can be one of the following (K.13.XX only):

- `undetermined USB reseat requirement`
- `USB reseat not required`
- `USB device reseat required for USB autorun`

The autorun feature only works when a USB device is inserted and the USB port is enabled.

Behavior of Autorun When USB Port is Disabled. Software Versions K.13.XX Operation. When using software version K.13.58, if the USB port is disabled (no usb-port command), the USB autorun function does not work in the USB port until the USB port is enabled, the config file is saved, and the switch is rebooted. The 5 volt power to the USB port remains on even after the USB port has been disabled.

For software versions after K.13.58, the 5 volt power applied to the USB port is synchronized with the enabling of the USB port, that is, when the USB port is enabled, the 5 volts are supplied; when the USB port is disabled, the 5 volts are not supplied. For previous software versions the power was supplied continuously. The autorun function does not require a switch reboot, but the USB device must be inserted at least once after the port is enabled so that the switch recognizes that the device is present. If the USB device is inserted and then the USB port is enabled, the switch does not recognize that a USB device is present.

Software Version K.14.XX Operation. For software versions K.14.XX, the USB port can be disabled and enabled without affecting the autorun feature. When the USB port is enabled, the autorun feature activates if a USB device is already inserted in the USB port.

Power is synchronized with the enabling and disabling of USB ports as described above for K.13.59 and later K.13.XX software versions, and K.14.31 and later K.14.XX software versions.

SNMP Implementation. The HP enterprise MIB hpicfUSBPort.mib allows configuration of the USB port with SNMP.

```
HP-ICF-USBPORT DEFINITIONS ::= BEGIN

IMPORTS
  OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY
    FROM SNMPv2-SMI
  NOTIFICATION-GROUP, OBJECT-GROUP, MODULE-COMPLIANCE
    FROM SNMPv2-CONF
  hpSwitch
    FROM HP-ICF-OID;

hpicfUSBPortMIB MODULE-IDENTITY
  LAST-UPDATED "200812180000Z"
  ORGANIZATION "Hewlett-Packard Company,
          Workgroup Networks Division"
  CONTACT-INFO "Hewlett Packard Company
          8000 Foothills Blvd.
          Roseville, CA 95747"
  DESCRIPTION "This MIB module manages the USB Port."

  --
  -- Revision History
  --

  REVISION    "200812180000Z"       -- December 18, 2008
  DESCRIPTION  "Add hpicfUSBPortZeroPowerStatus object "

  REVISION    "200809170000Z"       -- September 17, 2008
  DESCRIPTION  "Move NOTIFICATIONS OID from 3 to 0"

  REVISION    "200809100000Z"       -- September 10, 2008
  DESCRIPTION  "Added NOTIFICATIONS for enabled/disabled"

  REVISION    "200806250000Z"       -- June 25, 2008
  DESCRIPTION   "Original version"
```

```
    ::= { hpSwitch 53 }

  -- USBPort Configuration

  hpicfUSBPortConfig    OBJECT IDENTIFIER ::= { hpicfUSBPortMIB 1 }

  hpicfUSBPortStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                  notPresent(0),
                  enabled(1),
                  disabled(2) }

    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "hpicfUSBPortStatus control whether or not
              the USB port is enabled.
                notPresent(0)  - USBPort is not present
                enabled(1)  - USBPort Enabled.
                disabled(2) - USBPort Disabled.
             "
    DEFVAL { enabled }
    ::= { hpicfUSBPortConfig 1 }

   hpicfUSBPortZeroPowerStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                  powerUnavailable(0),
                  powerOff(1),
                  powerOn(2) }

    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "hpicfUSBPortZeroPowerStatus indicates if
              the USB port zero power is on or off.
                powerUnavailable(0)  - USBPort power reading is
                                       unavailable.
                powerOff(1)  - USBPort power is off.
                powerOn(2)   - USBPort power is on.
             "
    DEFVAL { powerOn }
    ::= { hpicfUSBPortConfig 2 }

   -- Notifications
  hpicfUSBPortNotifications OBJECT IDENTIFIER ::= { hpicfUSBPortMIB 0 }

  hpicfUSBPortEnabled NOTIFICATION-TYPE
    STATUS            current
    DESCRIPTION
          "An hpicfUSBPortEnabled notification signifies that the
           SNMP entity, acting in an agent role, has detected that
           the hpicfUSBPortStatus object has transitioned into the
           'enabled' state."
    ::= { hpicfUSBPortNotifications 1 }

  hpicfUSBPortDisabled NOTIFICATION-TYPE
    STATUS            current
    DESCRIPTION
```

```
        "An hpicfUSBPortDisabled notification signifies that the
         SNMP entity, acting in an agent role, has detected that
         the hpicfUSBPortStatus object has transitioned into the
         'disabled' state."
  ::= { hpicfUSBPortNotifications 2 }

-- USBPort conformance information

 hpicfUSBPortConformance
   OBJECT IDENTIFIER ::= { hpicfUSBPortMIB 2 }

 hpicfUSBPortGroups
  OBJECT IDENTIFIER ::= { hpicfUSBPortConformance 1 }

 hpicfUSBPortBaseGroup OBJECT-GROUP
   OBJECTS    {
              hpicfUSBPortStatus,
              hpicfUSBPortZeroPowerStatus
             }
   STATUS     current
   DESCRIPTION "A mandatory group with an object to enable
              or disable the USB port."
   ::= { hpicfUSBPortGroups 1 }

   hpicfUSBPortNotificationGroup NOTIFICATION-GROUP
     NOTIFICATIONS {
                 hpicfUSBPortEnabled,
                 hpicfUSBPortDisabled
                }
     STATUS     current
     DESCRIPTION "The hpicfUSBPort MIB Notification Group."
     ::= { hpicfUSBPortGroups 2 }

 -- USBPort conformance statements

 hpicfUSBPortCompliances
   OBJECT IDENTIFIER ::= { hpicfUSBPortConformance 2 }
 hpicfUSBPortCompliance MODULE-COMPLIANCE
   STATUS     current
   DESCRIPTION "Compliance statement for HP ICF USBPort
              configuration"
   MODULE
     MANDATORY-GROUPS { hpicfUSBPortBaseGroup,
                        hpicfUSBPortNotificationGroup }
   ::= { hpicfUSBPortCompliances 1 }

 END
```

- **Enhancement (PR_0000016100)** — A Global MAC Auth Password is now supported.

MAC Authentication Global Password

MAC authentication only requires that an entry is placed in the user database with the device's MAC address as both the username and the password, creating the opportunity for malicious device spoofing using the readily available MAC address. To make spoofing more difficult, the global password option allows a network administrator to configure a common MAC authentication password that is used for all MAC authentications sent to the RADIUS server.

Configuring the Global MAC Authentication Password. When implementing the global MAC authentication password option, it is important that the user database on the RADIUS server has the MAC authentication password as the password for each device performing MAC authentication.

Use this command to configure the global MAC authentication password.

Syntax: [no] aaa port-access mac-based password <***password-value***>

Specifies the global password to be used by all MAC authenticating devices.

The **no** *form of the command disables the feature.*

```
ProCurve(config)# aaa port-access mac-based password secretMAC1

ProCurve(config)# show port-access mac-based config

 Port Access MAC-Based Configuration

  MAC Address Format : no-delimiter
  Password           : secretMAC1


  Unauth Redirect Configuration URL :

  Unauth Redirect Client Timeout (sec) : 1800
  Unauth Redirect Restrictive Filter : Disabled
  Total Unauth Redirect Client Count : 0

                Client Client Logoff    Re-Auth   Unauth   Auth     Cntrl
  Port  Enabled Limit  Moves  Period    Period    VLAN ID  VLAN ID  Dir
  ----- -------- ------ ------ --------- --------- -------- -------- -----
  1     No       1      No     300       0         0        0        both
  2     No       1      No     300       0         0        0        both
  3     No       1      No     300       0         0        0        both
  4     No       1      No     300       0         0        0        both
  5     No       1      No     300       0         0        0        both
  6     No       1      No     300       0         0        0        both
  7     No       1      No     300       0         0        0        both
  8     No       1      No     300       0         0        0        both
```

Figure 46. Example of Configuring a Global MAC Authentication Password

Note The password value will display in an exported config file when **include-credentials** is enabled.

- **Enhancement (PR_0000040203)** — Support is added for the HP ProCurve 3500-24 (J9470A), 3500-24-PoE (J9471A), 3500-48 (J9472A), and 3500-48-PoE (J9473A) Switches.

Release K.14.32 Enhancements

- **Enhancement (PR_0000039363)** — Support is added for the "B" version of HP ProCurve SFP+ Direct Attach Cables (DAC) listed below. The "B" version DACs are compliant with the January 2009 version of the Multi-Source Agreement (MSA), SFF-8472 Rev 10.4. Additionally, the "B" version DACs interoperate with the Intel NIC (Intel 10 Gigabit AF DA Dual Port Server Adapter).
  - J9281B HP ProCurve 10-GbE SFP+ 1m Cable
  - J9283B HP ProCurve 10-GbE SFP+ 3m Cable
  - J9285B HP ProCurve 10-GbE SFP+ 7m Cable

Release K.14.34 Enhancements

- **Enhancement (PR_0000042932)** — Support is added for the following new products.
  - J9475A - HP ProCurve 8206zl Switch Base System
  - J9307A - HP ProCurve 24-Port 10/100/1000 PoE+ zl Module
  - J9308A - HP ProCurve 20-Port 10/100/1000 PoE+/4-port MiniGBIC zl Module
  - J9478A - HP ProCurve 24-port 10/100 PoE+ zl Module
  - J9447A - HP ProCurve 5406zl-48G-PoE+ Switch
  - J9448A - HP ProCurve 5412zl-96G-PoE+ Switch

Release K.14.35 Enhancements

- **Enhancement (PR_0000042908)** — Support is added for the following new products.
  - J9443A - HP ProCurve 630 Redundant/External Power Supply
  - J9309A - HP ProCurve 4-Port 10Gbe SFP+ zl Module

Release K.14.37 Enhancements

Release K.14.37 includes the following enhancements. (Not a public release)

- **Enhancement (PR_0000040368)** — Support is added for the following new products.
  - J9300A - HP ProCurve 10-GbE XFP-SFP+ 1m Direct Attach Cable
  - J9301A - HP ProCurve 10-GbE XFP-SFP+ 3m Direct Attach Cable
  - J9302A - HP ProCurve 10-GbE XFP-SFP+ 5m Direct Attach Cable
- **Enhancement (PR_0000016944)** — Log OSPF Adjacency Changes.

Log OSPF Adjacency Changes

In order to easily track adjacency changes among OSPF peers routers without enabling OSPF debug, event log messages will be generated on the OSPF router. The messages will indicate the formation and loss of adjacencies with peer routers. The output of the event log messages is minimal compared to OSPF debug output, and the event logs can be redirected to a syslog server that allows examination of the logs at a remote destination.

Configuring the Log Adjacency Option

Use the following command in ospf context to activate or deactivate the logging of OSPF neighbor adjacency changes. To enter ospf context, enable ip routing, and then enter the command **router ospf**.

Syntax: [no] logging neighbor-adjacency [detail]

Activates the logging of OSPF neighbor adjacency changes. The logs indicate the neighbor OSPF router interface moving into or out of the FULL state.

The **no** *version of the command deactivates the logging of OSPF neighbor adjacency changes.*

Default: The OSPF neighbor adjacency changes are logged by default. The **detail** *option is not enabled by default.*

[detail]: *When the optional* **detail** *parameter is configured, all state changes of the neighbor OSPF router interface are logged, not just those that occur when a neighbor goes up or down.*

```
ProCurve(ospf)# logging neighbor-adjacency detail
```

Figure 47. Example of Command for Logging OSPF Neighbor Adjacency Changes with detail Option

To display the configuration of logging neighbor adjacency changes, use the **show ip ospf general** command. The configuration displays as shown in Figure 48. The possible states are Enabled, Enabled with Detail, and Disabled.

```
ProCurve(ospf)# show ip ospf general

 OSPF General Status

  OSPF protocol           : enabled
  Router ID               : 15.255.133.27
  RFC 1583 compatability  : compatible

  Intra-area distance     : 110
  Inter-area distance     : 110
  AS-external distance    : 110

  Default import metric      : 10
  Default import metric type : external type 2

  Area Border               : yes
  AS Border                 : yes
  External LSA Count        : 9
  External LSA Checksum Sum : 408218
  Originate New LSA Count   : 24814
  Receive New LSA Count     : 14889
  Log Neighbor Adjacency Changes : Enabled with Detail
```

Logging of neighbor adjacency changes is enabled with the **detail** option.

Figure 48. Example of OSPF Information with the Status of Log Neighbor Adjacency Changes

Displaying in the Config File. The config file does not display information about logging neighbor adjacency changes when the feature is enabled, as that is the default configuration. When logging neighbor adjacency changes is disabled, or when it is enabled with the **detail** option, the information is shown in the config and running-config file.

```
ProCurve(ospf)# show run

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.XX

hostname "ProCurve Switch"
qos dscp-map 001111 priority 5
module 1 type J86xxA
ip routing
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-5,7,10-24
   ip address dhcp-bootp
   no untagged 6,8-9
   ip igmp
   exit
vlan 10
   name "VLAN10"
   untagged 8-9
   ip address 10.10.10.10 255.255.255.0
   exit
qos type-of-service diff-services
ip source-interface syslog 10.10.10.5
router ospf
   no logging neighbor-adjacency
   exit
```

Logging neighbor adjacency changes is disabled.

Figure 49. Example of Running Config File when Logging Neighbor Adjacency Changes is Disabled

Log Messages. The log messages seen when this feature is enabled are shown below.

Log Message	Description
OSPF: Nbr with Router ID <***router-id***>, IP address <***ip-addr***> moved to FULL state - adjacency formed	Logged when an adjacency is formed.
OSPF: Nbr with Router ID <***router-id***>, IP address <***ip-addr***> moved out of FULL state - adjacency lost.	Logged when an adjacency is lost.
OSPF: Nbr with Router ID <***router-id***>, IP address <***ip-addr***> moved in to INITIALIZE/EXSTART/EXCHANGE/LOADING state.	When the **detail** option is used, all neighbor state transitions are logged.

Release K.14.40 Enhancements

Release K.14.40 includes the following enhancements. (Not a public release)

- **Enhancement (PR_0000016237)** — Port VLAN ID TLV Support on LLDP.

Port VLAN ID TLV Support on LLDP

The **port-vlan-id** option enables advertisement of the port VLAN ID TLV as part of the regularly advertised TLVs. This allows discovery of a mismatch in the configured native VLAN ID between LLDP peers. The information is visible using **show** commands and will be logged to the Syslog server.

Configuring the VLAN ID TLV. This TLV advertisement is enabled by default. To enable or disable the TLV, use this command.

Syntax: [no] lldp config <port-list> dot1TlvEnable port-vlan-id

Enables the VLAN ID TLV advertisement. The **no** *form of the command disables the TLV advertisement.*

Default: Enabled.

```
ProCurve(config)# lldp config a1 dot1TlvEnable port-vlan-id
```

Figure 50. Example of Enabling the VLAN ID TLV

Displaying the TLVs Advertised. The show commands display the configuration of the TLVs. The command **show lldp config** lists the TLVs advertised for each port.

```
ProCurve(config)# show lldp config a1

 LLDP Port Configuration Detail

  Port : a1
  AdminStatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False


  TLVS Advertised:
   * port_descr
   * system_name
   * system_descr
   * system_cap

   * capabilities
   * network_policy
   * location_id
   * poe

   * macphy_config

   * port_vlan_id   <-- The VLAN ID TLV is being advertised.

  IpAddress Advertised:
     :
     :
```

Figure 51. Displaying the TLVs for a Port

```
ProCurve(config)# show lldp info local-device a1

LLDP Local Port Information Detail

  Port     : A1
  PortType : local
  PortId   : 1
  PortDesc : A1

  Port VLAN ID : 1   <-- The information that LLDP used in its advertisement.
```

Figure 52. Example of Local Device LLDP Information

```
ProCurve(config)# show lldp info remote-device a1

LLDP Remote Device Information Detail

  Local Port   : A1
  ChassisType  : mac-address
  ChassisId    : 00 16 35 22 ca 40
  PortType     : local
  PortId       : 1
  SysName      : esp-dback
  System Descr : ProCurve J8693A Switch 3500yl-48G, revision K.13.03, ROM ...
  PortDescr    : A1

  System Capabilities Supported  : bridge, router
  System Capabilities Enabled    : bridge, router

  Port VLAN ID : 200

  Remote Management Address
     Type    : ipv4
     Address : 192.168.1.1
```

Figure 53. Example of Remote Device LLDP Information

SNMP Support. The LLDP-EXT-DOT1-MIB has the corresponding MIB variables for the Port VLAN ID TLV. The TLV advertisement can be enabled or disabled using the MIB object **lldpXdot1ConfigPortVlanTxEnable** in the **lldpXdot1ConfigPortVlanTable**.

The port VLAN ID TLV local information can be obtained from the MIB object **lldpXdot1LocPortVlanId** in the local information table **lldpXdot1LocTable**.

The port VLAN ID TLV information about all the connected peer devices can be obtained from the MIB object **lldpXdot1RemPortVlanId** in the remote information table **lldpXdot1RemTable**.

- **Enhancement (PR_0000040732)** — Remote Mirroring Using the Loopback Interface.

Remote Mirroring Using the Loopback Interface

This enhancement allows the use of a switch loopback IP address as the destination address when configuring remote mirroring. A loopback IP address can also be used as a source address. Configuring the destination IP address as a loopback address allows remote mirroring to continue if a port or VLAN goes down. The ports that are still up continue to have the traffic analyzed.

Any configured loopback address can be used except the switch's default loopback address of 127.0.0.1.

The following illustration shows a basic topology that could be used for remote mirroring.

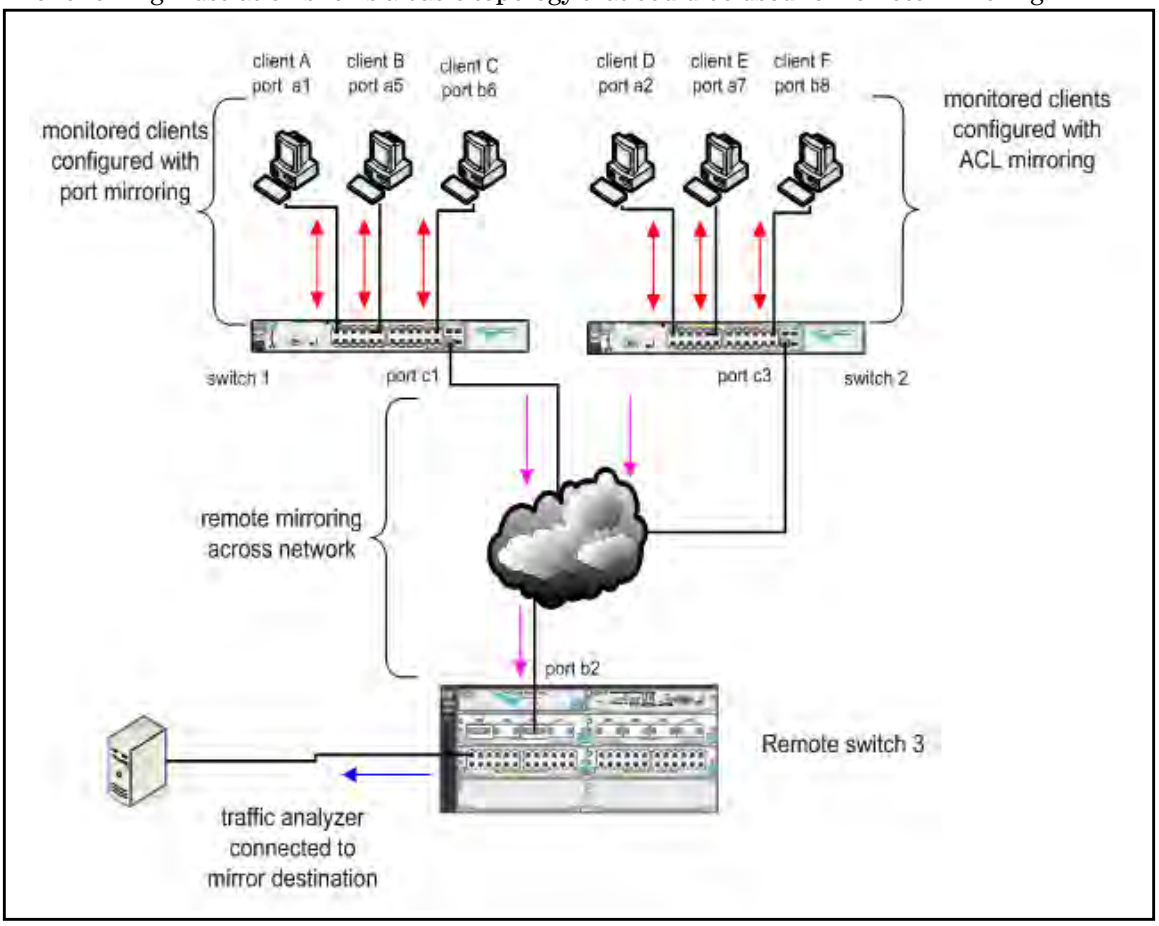


Figure 54. Example of Remote Mirroring

Configuring Remote Mirroring. It is advisable to configure the remote destination IP address first. To configure the remote destination IP address, use the following command:

Syntax: mirror endpoint ip <src-ip-addr> <src-udp-port> <dst-ip-addr> port <port-num>

Configure a mirror port for diagnostic purposes. The network traffic seen by the monitored ports (defined with "monitor" command) is copied to the mirror port to which an network analyzer can be attached.

When mirroring multiple ports in high traffic, some frames may not be copied to the monitoring port.

Note: The source IP address, source UDP port, and destination IP address specified on the source switch must match those on the respective destination switch.

Note: You must use the **endpoint** *keyword when using the* **no** *form of the command with src-ip-addr, src-udp-port and dst-ip-addr.*

<src-ip-addr>: source IP address for remote mirroring

<src-udp-port>: source UDP port for remote mirroring

<dst-ip-addr>: destination IP address for remote mirroring

For example:

- Loopback address 3.3.3.3 is configured on switch 3
- Switch 1, port C1 has IP address 10.11.12.1 configured

To configure switch 1 to encapsulate the traffic from mirror session 2 using loopback address 10.11.12.1, source UDP port 345 and destination IP address 3.3.3.3, enter the following commands:

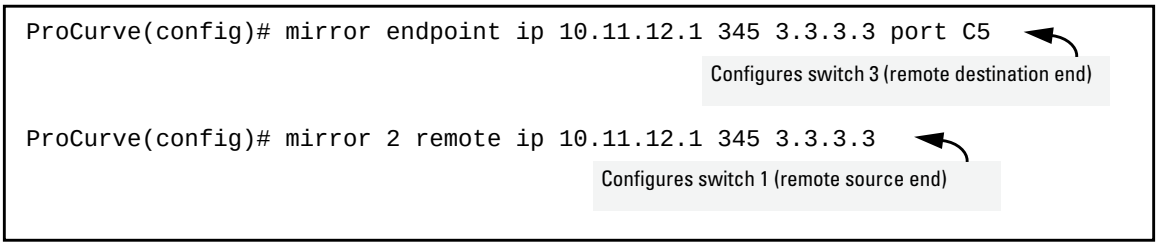


Figure 55. Example of Configuring a Loopback IP Address for the Destination IP Address

You can also use a loopback IP address for the remote source end.

Syntax: mirror <1-4> [name <name-str>] remote ip <src-ip-addr> <src-udp-port> <dst-ip-addr>

Define the mirror port for diagnostic purposes.

The source IP address and destination IP address may be any valid address, including the loopback addresses except the default loopback address 127.0.0.1.

<1-4>: Mirror destination number

name <name-str>: Friendly name to be associated with the mirror destination number.

For example:

- Loopback address 4.4.4.4 is configured on switch 1
- Switch 3, port B2 has an IP address of 10.11.12.13

To configure switch 1 to encapsulate the traffic from mirror session 2 with a loopback address of 4.4.4.4, a source UDP port of 345, and a destination IP address of 10.11.12.13, enter the following commands:

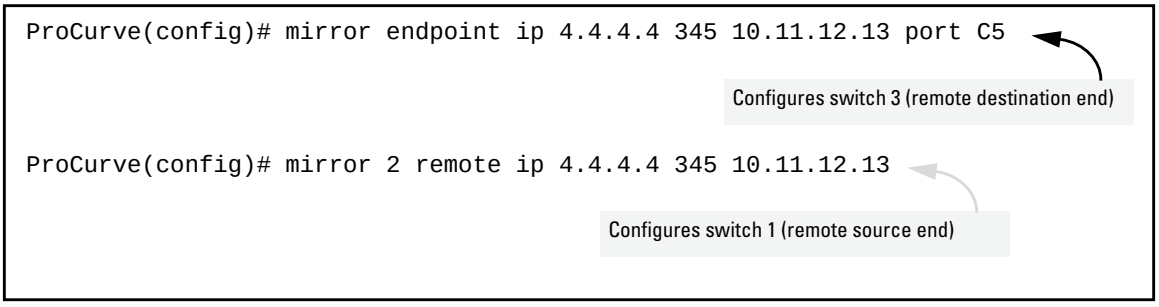


Figure 56. Example of Configuring a Loopback IP Address for the Source IP Address

- **Enhancement (PR_0000038122)** — TELNET Negotiate About Window Size (NAWS) Initiation.

Telnet Negotiate About Window Size (NAWS) Initiation

When a telnet connection is established with a switch, the switch always uses the default values of 80 columns by 24 lines for the window dimensions. The window can be resized by either dragging the corner of the window, or by executing the **terminal length <x> width <y>** CLI command and then configuring the telnet client with those dimensions. The new window dimensions are lost after that telnet session ends.

When the telnet connection is established with an HP switch, either the switch or the telnet client needs to initiate the inquiry about the availability of NAWS. If NAWS is available, you can resize the window by dragging the corner of the window to the desired size. The telnet software uses NAWS to tell the switch what the new window dimensions are. If the switch supports the requested window dimensions, it uses them for all future interactions. If the switch does not support those window dimensions, it refuses them and the telnet client requests an alternate set of window dimensions. The negotiation continues until the telnet client and the switch agree on the window dimensions.

Making Window Size Negotiation Available for a Telnet Session. The switch currently responds to a request from the remote telnet client to negotiate window size. However, some telnet clients do not request to negotiate window size unless the switch's telnet server suggests that NAWS is available.

This update allows window size negotiation to occur with telnet clients that support NAWS but do not try to use it unless it is suggested by the switch's telnet server. The switch's telnet server will suggest to the telnet client that NAWS is available.

- **Enhancement (PR_0000042815)** — When a config is uploaded to the switch containing a banner MOTD configuration that exceeds the maximum multi-line input, the following error message is now returned at the CLI: `Only 16 lines allowed in multi-line input.  Command not executed`.
- **Enhancement (PR_0000043278)** — Crash information was improved in order to speed time to resolution.
- **Enhancement (PR_0000018513)** — Banner enhancements were made.

Banner Enhancements

The enhancements to the Message of The Day (MOTD) banner apply to the following authentication types:

- Local
- RADIUS
- TACACS

The enhancements are:

- The MOTD banner size is increased to 1280 characters.
- If the MOTD is configured, the copyright, switch identification, and software version are not displayed on the splash screen; only the customer-defined banner is displayed.
- When passwords are configured on the switch, there will not be a prompt to "press any key to continue". This prompt will still appear if a password is not configured.

Example Banner Configurations. Default Banner with No Password Configured. When the MOTD is not configured and there is no password, the default login page displays. The information includes the switch identification, software version, copyright statement and default banner. The "press any key to continue" prompt displays. When any key is pressed, the banner is cleared and the CLI prompt displays.

Default Banner with Password Configured. When passwords are configured on the switch, but the MOTD is not configured, the default login page displays. A prompt for the password appears. After a correct password is entered, the default banner clears and the CLI prompt displays.

Customized Banner without Password Configured. When a custom MOTD banner is configured and there is no password required, the custom MOTD banner displays followed by the "press any key to continue" prompt. When any key is pressed, the custom banner is cleared and the CLI prompt displays.

Customized Banner with Password Configuration. When a custom MOTD banner is configured on the switch and a password is required, the custom banner displays, followed by the password prompt. Entering the correct password clears the banner and displays the CLI prompt.

- **Enhancement (PR_0000040021)** — A Source IP Identity may now be configured for SNTP, outgoing TELNET and TFTP.

Single Source IP Identity

This enhancement applies to the following software applications:

- RADIUS
- SNTP
- System Logging applications
- TACACS
- Telnet
- TFTP

The above IP-based software applications use a client-server communication model, that is, the client's source IP address is used for unique client identification. The source IP address is determined by the system and is usually the IP address of the outgoing interface in the routing table. However, routing switches may have multiple routing interfaces due to load balancing or routing redundancy, and outgoing packets can potentially be sent by different paths at different times. This results in different source IP addresses, which creates a client identification problem on the server site. For example, there is no way to designate a fixed IP address for outgoing packets for RADIUS or TACACS, so it is necessary to configure in the RADIUS or TACACS database all possible IP addresses that are configured on the switch as valid clients. When using system logging, it can be difficult to interpret the logging and accounting data on the server site as the same client can be logged with different IP addresses.

To decrease the amount of administrative work involved, a configuration model is provided that allows the selection of an IP address to use as the source address for all outgoing traffic generated by a specified software application on the switch. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server.

Specifying the Source IP Address. The CLI command **ip source-interface** is used to specify the source IP address for an application. Different source IP addresses can be used for different software applications, but only one source IP address can be specified for each application.

Syntax: [no] ip source-interface <radius | tacacs | telnet | tftp | sntp | syslog | all> <loopback <***id***> | vlan <***vlan-id***> <***ip-address***>>

Determines the source IP address used by the specified software application when transmitting IP packets. The **all** *parameter can be used to set one IP address for all the listed applications.*

The **no** *version of the command cancels the configuration and the application reverts to its default behavior. The system determines the source IP address of outgoing application-specific IP packets at packet transmission time.*

loopback <*id*>: *Specifies that the IP address of the loopback interface is used as the source IP address in outgoing packets. If the loopback interface has no IP address, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

vlan <*vlan-id*>: *Specifies that the IP address of the indicated VLAN interface is used as the source IP address of outgoing packets. If the specified VLAN interface has no IP address configured, or is down, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

<*ip-address*>: *Specifies the IP address that should be used as the source IP address of outgoing packets. The IP address must be a valid IP address configured on one of the switch's VLAN or loopback interfaces. If the interface is down, then the application reverts to the default behavior.*

The Source IP Selection Policy. The source IP address selection for the application protocols is defined through assignment of one of the following policies:

- Outgoing Interface—the IP address of the outgoing IP interface is used as the source IP address. This is the default policy and the default behavior of applications.
- Configured IP Address—the specific IP address that is used as the source IP address. This address is configured on one of the switch's IP interfaces, either a VLAN interface or a Loopback interface.
- Configured IP Interface—the IP address from the specific IP interface (VLAN or Loopback) is used as the source IP address. If there are multiple IP addresses assigned (multinetting, for example), the lowest IP address is used.

If the selection policy cannot be executed because the interface does not have an IP address configured, does not exist, or is down, the application protocol uses the default Outgoing Interface policy. A warning message is displayed, but the configuration changes are accepted. When using the **show ip source-interface status** command to display information about the source IP address selection policy, the administratively-assigned source IP selection policy and the actual (operational) source IP selection policy in effect are displayed. The operational source IP selection policy may be different from the assigned source selection policy if the IP interface does not exist or is down. In this case, the default of Outgoing Interface appears as the operational policy. See Figure 57.

```
ProCurve (config)# show ip source-interface detail

 Source-IP Detailed Information

  Protocol : Tacacs
  Admin Policy           : Configured IP Interface
  Oper Policy            : Outgoing Interface
  Source IP Interface    : Vlan 22
  Source IP Address      : 10.10.10.4
  Source Interface State : Down
```

The Admin Policy differs from the Oper Policy because the Source Interface State is Down. The default Outgoing Interface policy is actually in effect.

Figure 57. Example of the Administratively-assigned Source IP Selection Policy Differing From the Operational Policy

The **no** form of the **ip source-interface** command reverts the application protocols to the default behavior. The Outgoing Interface policy is used.

Figure 58 is an example of assigning a specific source IP address for a RADIUS application. The administrative policy is Configured IP Address.

```
ProCurve(config)# ip source-interface radius 10.10.10.2

ProCurve(config)# show ip source-interface radius

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Radius   | Configured IP Address                 10.10.10.2
```

Figure 58. Example of a Specific IP Address Assigned for the RADIUS Application Protocol

In Figure 59, a VLAN interface (VLAN 22) is specified as the source IP address for TACACS. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface tacacs vlan 22

ProCurve(config)# show ip source-interface tacacs

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Tacacs   | Configured IP Interface vlan 22
```

Figure 59. Example of Using a VLAN Interface as the Source IP Address for TACACS

Figure 60 shows a VLAN interface being specified as the source IP address for logging. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface syslog vlan 10

ProCurve(config)# show ip source-interface syslog

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Syslog   | Configured IP Interface vlan 10
```

Figure 60. Example of Using a VLAN Interface as the Source IP Address for Logging (Syslog)

Displaying the Source IP Interface Information. There are several **show** commands that can be used to display information about the source IP interface status.

Syntax: show ip source-interface status [radius | sntp | tacacs | telnet | tftp | syslog]

Displays the operational status information for the source IP address selection policy. Both the administratively-assigned source IP selection policy and the operational source IP selection policy are displayed.

When no parameters are specified, policy information for all protocols is displayed.

```
ProCurve(config)# show ip source-interface status

 Source-IP Status Information

  Protocol | Admin Selection Policy  Oper Selection Policy
  -------- + ---------------------- ----------------------
  Tacacs   | Configured IP Interface Configured IP Interface
  Radius   | Configured IP Address   Configured IP Address
  Syslog   | Configured IP Interface Outgoing Interface
  Telnet   | Outgoing Interface      Outgoing Interface
  Tftp     | Outgoing Interface      Outgoing Interface
  Sntp     | Outgoing Interface      Outgoing Interface
```

Figure 61. Example of the Data Displayed for Source IP Interface Status

When executing the **show ip source-interface** command without parameters, the configured IP interfaces (VLANs) and IP addresses are displayed for each protocol.

```
ProCurve(config)# show ip source-interface

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Tacacs   | Configured IP Interface vlan 22
  Radius   | Configured IP Address                  10.10.10.2
  Syslog   | Configured IP Interface vlan 10
  Telnet   | Outgoing Interface
  Tftp     | Outgoing Interface
  Sntp     | Outgoing Interface
```

Figure 62. Example of show ip source-interface Command Output

The **show ip source-interface detail** command displays detailed information about the configured policies, source IP address, and interface state for each protocol.

Syntax: show ip source-interface detail [radius | sntp | tacacs | telnet | tftp | syslog]

Displays detailed operational status information for the source IP address selection policy. Information about the configured policies, source IP address and interface state are displayed.

When no parameters are specified, policy information for all protocols is displayed.

```
ProCurve(config)# show ip source-interface detail

 Source-IP Detailed Information

  Protocol : Tacacs
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : vlan 22
  Source IP Address      : 10.10.10.4
  Source Interface State : Up

  Protocol : Radius
  Admin Policy           : Configured IP Address
  Oper Policy            : Configured IP Address
  Source IP Interface    : vlan 3
  Source IP Address      : 10.10.10.2
  Source Interface State : Up

  Protocol : Syslog
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : vlan 10
  Source IP Address      : 10.10.10.10
  Source Interface State : Up

  Protocol : Telnet
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : loopback 1
  Source IP Address      : 10.10.10.11
  Source Interface State : Up

  Protocol : Tftp
  Admin Policy           : Outgoing Interface
  Oper Policy            : Outgoing Interface
  Source IP Interface    : N/A
  Source IP Address      : N/A
  Source Interface State : N/A

  Protocol : Sntp
  Admin Policy           : Outgoing Interface
  Oper Policy            : Outgoing Interface
  Source IP Interface    : N/A
  Source IP Address      : N/A
  Source Interface State : N/A
```

Figure 63. Example of Detailed Information Displayed for Each Protocol

The **show** command can also be used with the application to display the source IP address selection information in effect for the application protocol.

```
ProCurve(config)# show radius

Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :
  Dynamic Authorization UDP Port : 3799
  Source IP Selection : Configured IP address
```

Source IP Selection for the specified application protocol is displayed.

Figure 64. Example of show radius Command Displaying Source IP Selection Information

```
ProCurve(config)# show tacacs

 Status and Counters - TACACS Information

  Timeout : 5
  Source IP Selection : Configured IP Interface
  Encryption Key :
```

Source IP Selection for the specified application protocol is displayed.

Figure 65. Example of show tacacs Command Displaying Source IP Selection Information

```
ProCurve(config)# show debug

Debug Logging

  Source IP Selection: Configured IP interface
  Destination:    None

  Enabled debug types:
   None are enabled.
```

Source IP Selection for the specified application protocol is displayed.

Figure 66. Example of show debug Command Displaying Source IP Selection Information for Syslog

```
ProCurve(config)# show telnet

 Telnet Activity

 Source IP Selection: 10.10.10.11

 ----------------------------------------------------
 Session  : **  1
 Privilege: Manager
 From     : Console
 To       :
```

Source IP Selection is displayed.

Figure 67. Example of show telnet Command Displaying Source IP Selection

```
ProCurve(config)# show sntp

 SNTP Configuration

  SNTP Authentication : Disabled
  Time Sync Mode: Timep
  SNTP Mode : disabled
  Poll Interval (sec) [720] : 720
  Source IP Selection: Outgoing Interface
```

Source IP Selection is displayed.

Figure 68. Example of show sntp Command Displaying Source IP Selection

Error Messages. The following error messages may appear when configuring source IP selection if the interface does not exist, is not configured for IP, or is down.

Error Message	Description
Warning: Specified IP address is not configured on any interface	The IP address specified has not been assigned to any interface on the switch.
Warning: Specified IP interface is not configured	The IP interface has not been configured.
Warning: Specified IP interface is not configured for IP	An IP address has not been assigned to this interface.
Warning: Specified IP interface is down	The interface on the switch associated with this IP address is down.
Warning: Specified IP interface is configured for DHCP	The IP address has not been configured specifically (manually) for this interface and may change.

- **Enhancement (PR_0000040721)** — Extended ping and traceroute are now available.
- **Enhancement (PR_0000040378)** — Implementation of DHCP hostname (option 12).

DHCP Option 12

CLI Command

This feature allows you to include the hostname in the DHCP packet sent to the DHCP server. This is disabled by default. The command must be executed from the global configuration level.

Syntax: [no] dhcp host-name-option

Sends the hostname option with DHCP packets. Use the **no** *form of the command to not include the hostname in the packet.*

The maximum size of the hostname is 32 characters.

Default: Disabled

```
ProCurve(config)# dhcp host-name-option
```

Figure 69. Example of the DHCP Option 12 Command

SNMP Support. An MIB object supports enabling and disabling the DHCP Option 12 feature. It is added in the hpicfDhcp-client.mib. The hostname is retrieved from the MIB variable SYSNAME. Validity checks on the name include:

- The name starts with a letter, ends with a letter or a digit, and can have letters, hyphens, or digits in between the first and last characters.

- The maximum size supported for a hostname is 30 characters. If SYSNAME is more than 30 characters, then DHCP Option 12 will not be included in the packet.
- The minimum number of characters supported for a hostname is one character. If the SYSNAME in the MIB is null, then DHCP Option 12 will not be included in the packet.

SNMP MIB Definition. hpicfDhcpClientHostNameOption OBJECT-TYPE

```
SYNTAX          INTEGER {
                      enabled (1),
                      disabled (2)
                }
MAX-ACCESS   read-write
STATUS          current
                DESCRIPTION “This object enables/disables DHCP option 12
                that allows for sending of the system hostname in DHCP packets.
                By default, this object is set to be disabled”.

                Setting this flag to ‘enabled’ results in the inclusion
                of system hostname in DHCP packets.


DEFVAL  { disabled }

::= { hpicfDhcpClientOptions 2 }
```

- **Enhancement (PR_0000037664)** — DHCP-based Auto Image and Configuration Update.

DHCP-based Auto Image and Configuration Update

This enhancement provides a one-step approach for managing the remote download of the software image and the configuration file from the switch.

The following pre-requisites are required for the automatic image and configuration upload to work. Setting options 66 and 67 on a DHCP server allows a switch to boot from a default configuration to a specified configuration file.

1. One or more DHCP Servers are enabled and configured for the following DHCP options:
   - DHCP Option 66—Sets the TFTP server IP Address
   - DHCP Option 67—specifies the file name of the config file
   - DHCP Option 60—the Vendor Class Identifier, sent by the client for the server to process
   - DHCP Option 43—the Vendor Specific Information supplied by the DHCP server, which includes the image filename.
2. One or more TFTP servers are loaded with the configuration file and image file.

Note The DHCP options are only executed for the primary VLAN.

Configuring the Command for DHCP Options 66 and 67. To specify that DHCP Options 66 and 67 should be processed, enter the **dhcp config-file-update** command.

Syntax: [no] dhcp config-file-update

Enables the processing of DHCP Options 66 and 67.

Note: Option 66 is processed when either **dhcp config-file-update** *or* **dhcp image-file-update** *are configured.*

Use the **no** *form of the command to disable the processing of options 66 and 67.*

Configuring the Command for Vendor Specific Information (Option 43)

To request that the Vendor Specific Information is supplied by the DHCP server, enter the **dhcp vendor-specific** command.

Syntax: [no] dhcp vendor-specific

Requests that the Vendor Specific Information (DHCP Option 43) be supplied by the DHCP server, which includes the software image filename.

Use the **no** *form of the command to disable the processing of DHCP Option 43.*

Note: You cannot disable DHCP Option 43 while **dhcp image-file-update** *is enabled.*

Note If DHCP Option 43 is incorrectly specified or corrupt, it will be ignored when the DHCP packet is processed. The other DHCP options (60, 66, 67) are processed if they are present and correctly specified.

Enabling the Image File Update Process. To enable the image file update, use this command.

Syntax: [no] dhcp image-file-update

Enables image file update through DHCP. Image download on primary as well as secondary slots is supported. The currently active slot (primary or secondary) is the target of the new image downloaded via DHCP.

Note: This command overrides the existing **auto-tftp** *command, that is, unless this command is configured in the* **no** *form, auto-tftp will not be performed.*

Note: Option 66 is processed when either **dhcp config-file-update** *or* **dhcp image-file-update** *are configured.*

Use the **no** *form of the command to prevent file update using DHCP.*

Default: Enabled

```
ProCurve(config)# dhcp image-file-update
```

Figure 70. Example of the Image File Update Command

Displaying the Current Status of the DHCP Client. Displaying the Config File Update Status

To display the DHCP client's current config file update status, enter the command as shown in figure 71.

```
ProCurve(config)# show dhcp client config-file-update

Downloading Config File from TFTP server is enabled
```

Figure 71. Example of DHCP Options 66 and 67 Status as Enabled

Displaying the Vendor Specific Information Option Status (Option 43). To display the DHCP client's Vendor Specific Information option status, enter the command as shown in figure 72.

```
ProCurve(config)# show dhcp client vendor-specific

Vendor Class Id = ProCurve Switch
Processing of Vendor Specific Configuration is enabled
```

Figure 72. Example of DHCP Option 43 Status as Enabled

Displaying the Image File Update Status. To display the current status of the image file update feature, enter the command as shown in figure 73.

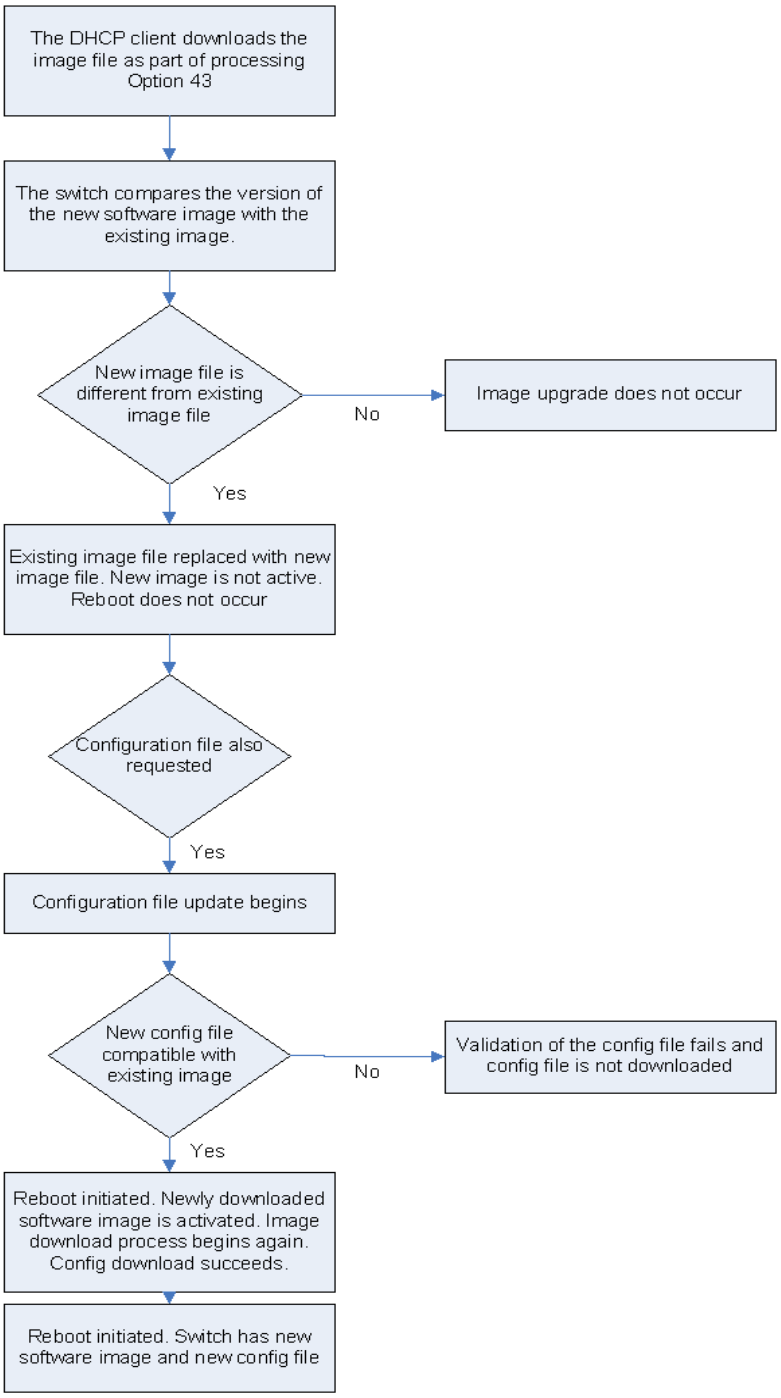
```
ProCurve(config)# show dhcp client image-file-update

Downloading Image File from TFTP server is disabled
```

Figure 73. Example of Image File Update Feature Status as Disabled

How the Files Are Downloaded. The downloading of the image file and the configuration file happens sequentially.

1. The DHCP client downloads the image file as part of processing DHCP option 43.
2. After downloading the file, the switch compares the version of the new software image file with the existing image file. If the new file is different from the existing file, the existing image file is replaced with the new image file. At this point the newly downloaded image is not the active image. A reboot does not immediately follow the image file replacement.
3. If the configuration file is also requested via DHCP options 66 and 67, the configuration file update begins. If the new configuration file is compatible with the existing image, the configuration download is successful and a reboot is initiated. The validation of the new configuration file may fail if the file contains an command that is ONLY supported by the newly downloaded image file, which is not yet active.
4. If the new configuration file is not compatible with the existing image, the configuration download fails and a reboot is initiated. The newly downloaded software image is activated.
5. When the switch is finished rebooting, the image download process begins again. The validation verifies that the active image on the switch and the one to be downloaded are the same image version. An image upgrade does not occur.
6. The configuration download will succeed now as the configuration file downloaded from the TFTP server is validated against the new software image active on the switch. This initiates a second reboot.
7. The switch now has the new software image and the new configuration file.

The following diagram illustrates the steps.


The DHCP client downloads the image file as part of processing Option 43
The switch compares the version of the new software image with the existing image.
New image file is different from existing image file
No
Image upgrade does not occur
Yes
Existing image file replaced with new image file. New image is not active. Reboot does not occur
Configuration file also requested
Yes
Configuration file update begins
New config file compatible with existing image
No
Validation of the config file fails and config file is not downloaded
Yes
Reboot initiated. Newly downloaded software image is activated. Image download process begins again. Config download succeeds.
Reboot initiated. Switch has new software image and new config file

Event Log Messages. The following messages may appear in the Event Log.

Message	Description
Image Download from <***ip-address***> initiated via DHCP	DHCP has initiated an image download form a TFTP server whose IP address is specified in the log message.
Config download from <***ip-address***> initiated via DHCP	DHCP has initiated a config download from a TFTP server whose IP address is specified in the log message.
Image-download via DHCP failed	The DHCP server is not reachable, the image file is not found, or the downloaded image file is corrupt.
Config-download via DHCP failed	The DHCP server is not reachable, the config file is not found, or the configured image file is corrupt.
Transfer timed out	The connection to the TFTP server timed out.
Transfer aborted, wrong file	The file format of the image file or the config file is incorrect.
Connection to <***ip-address***> failed	The client failed to connect to the TFTP server.
Tftp: Request failed	A generic error returned when the system resources are unavailable.
Transfer canceled. No workspace left on device.	The image is too big to fit in the RAM
Transfer Fatal Error. Hardware fault on device, Corrupt FLASH	The flash is corrupt and cannot be written to.
Transfer canceled. File too big to fit in FLASH	The download image size is greater than what can be accommodated in the flash.
Transfer completed	The transfer is completed. Occurs before validation begins.
Primary Image updated via network tftp/ Secondary Image updated via network tftp	Issued by TFTP after the image is written to flash depending on whether primary or secondary is updated.
Image download via DHCP Client is enabled. Disabling Auto-TFTP	DHCP is configured to fetch the image file. The auto TFTP feature is disabled to avoid any potential race condition to download the image.
Image file transfer and validation completed	The image file has been obtained from the TFTP server and the validation of the image is complete.
Config file transfer and validation is complete	The configuration file update has been obtained from the TFTP server and the validation of the config file is completed.

Release K.14.42 Enhancements

Release K.14.42 includes the following enhancements. (Not a public release)

- **Enhancement (PR_0000017201)** — The switch Fault Finder function has been extended to cover an improperly behaving fiber transceiver, or other condition which results in a link "flapping" rapidly between link-up and link-down states. A new fault event "link-flap" has been created to detect these events. Additionally, a new action, "warn-and-disable," has been created to report and disable the events. Together, these enhancements allow the errant condition to be detected, and the port in question optionally disabled.

Flapping Transceiver Mitigation

In ProCurve switches, the state of a link is driven directly by the reported state of the port, which is required for rapid detection of link faults. However, the consequence of this is that a marginal transceiver, optical, or wire cabling, one which “flaps” up and down several times per second, can cause STP and other protocols to react poorly, resulting in a network outage. This

enhancement expands the functionality of the existing Fault Finder function to include a “link-flap” event and a new action of "warn-and-disable". Together, these additions allow the errant condition to be detected, and the port in question can be optionally disabled.

Syntax: **fault-finder <link-flap> sensitivity <low | medium | high> action <warn | warn-and-disable>**

Default settings: **Sensitivity = Medium; Action = Warn**

Sensitivity thresholds are static. In a 10-second window, if more than the threshold number of link state transitions (up or down) is detected, the event is triggered. The 10-second window is statically determined, i.e. the counters are reset every 10 seconds, as opposed to being a sliding window. The counters are polled twice per second (every 500 milliseconds), and the event is triggered if the sensitivity threshold is crossed at that time.

The sensitivity thresholds are:

High = 3 transitions in 10 seconds

Medium = 6 transitions in 10 seconds

Low = 10 transitions in 10 seconds

Configuration of the link-flap event and corresponding action applies to all ports and port types (it is a global setting per FFI event type). Note that normal link transition protocols may prevent link state changes from occurring fast enough to trigger the event for some port types, configurations, and sensitivity settings.

When the link-flap threshold is met for a port configured for **warn** (e.g. **fault-finder link-flap sensitivity medium action warn**), the following message will be seen in the switch event log.

```
02672 FFI: port <number>-Excessive link state transitions
```

When the link-flap threshold is met for a port configured for warn-and-disable (e.g. **fault-finder linkflap sensitivity medium action warn-and-disable**), the following messages will be seen in the switch event log.

```
02672 FFI: port <number>-Excessive link state transitions
02673 FFI: port <number>-Port disabled by Fault-finder.
02674 FFI: port <number>-Administrator action required to re-enable.
```

The warn-and-disable action is available for all fault-finder events on an individual basis. It may be used, for example, to disable a port when excessive broadcasts are received. Because the fault-generated disabling of a port requires operator intervention to re-enable the port, such configuration should be used with care. For example, link-flap initiated disablement is not desired on ports that are at the client edge of the network, because link state changes there are frequent and expected.

Automatic disabling of a port when excessive broadcasts are detected is not recommended at the core or distribution layers, due to the potential to disable large parts of the network that may be uninvolved, and for the opportunity to create a denial-of-service attack.

Within the Web Management interface, double clicking an event on a port that was configured with warn-and-disable and has met the threshold to trigger the disable action, will bring up a dialog box with the event details. The event dialog box now contains a button at the bottom of the page, which can be used to re-enable the disabled port. The button will remain, even if the port has already been brought up through a prior exercise of it, or if the port was re-enabled via some other interface (e.g. the command line). Re-enabling an already enabled port has no effect. The button to acknowledge the event remains unchanged.

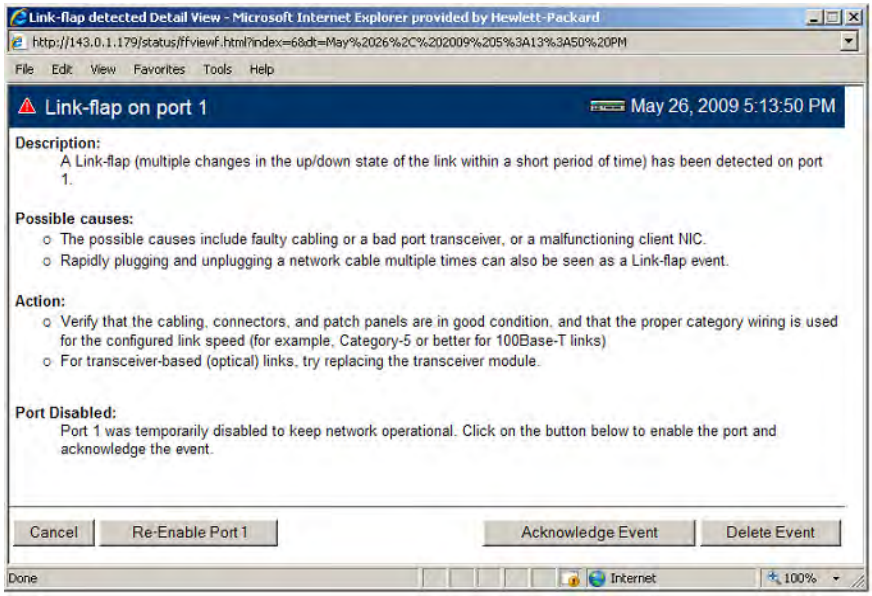


Figure 74. Link-flap on port 1 event detail dialog box

- **Enhancement (PR_ 0000045438)** — The Out Of Band Management (OOBM) port on the HP ProCurve Switch 6600 Series is now enabled for IPv6 host functionality.

Release K.14.43 Enhancements

Software never built.

Release K.14.44 Enhancements

Release K.14.44 includes the following enhancements. (Not a public release)

- **Enhancement (PR_0000041022)** —Enhancement to AAA accounting. For more information, see the following "Accounting Services" section.

Accounting Services

RADIUS accounting collects data about user activity and system events and sends it to a RADIUS server when specified events occur on the switch, such as a logoff or a reboot.

Accounting Service Types. The switch supports four types of accounting services:

- **Network accounting:** Provides records containing the information listed below on clients directly connected to the switch and operating under Port-Based Access Control (802.1X):
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Acct-Input-Packets
  - Acct-Output-Packets
  - Acct-Input-Octets
  - Nas-Port
  - Acct-Output-Octets
  - Acct-Session-Time
  - User-Name
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id

- **Exec accounting:** Provides records holding the information listed below about login sessions (console, Telnet, and SSH) on the switch:
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Acct-Session-Time
  - User-Name
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id

- **System accounting:** Provides records containing the information listed below when system events occur on the switch, including system reset, system boot, and enabling or disabling of system accounting.
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Delay-Time
  - NAS-IP-Address
  - NAS-Identifier

- **Commands accounting:** Provides records containing information on CLI command execution during user sessions.
  - Acct-Session-Id
  - Acct-Status-Type
  - Service-Type
  - Acct-Authentic
  - User-Name
  - NAS-IP-Address
  - NAS-Identifier
  - NAS-Port-Type
  - Calling-Station-Id
  - HP-Command-String
  - Acct-Delay-Time

The switch forwards the accounting information it collects to the designated RADIUS server, where the information is formatted, stored, and managed by the server. For more information on this aspect of RADIUS accounting, refer to the documentation provided with your RADIUS server.

Operating Rules for RADIUS Accounting. •You can configure up to four types of accounting to run simultaneously: exec, system, network, and command.

- RADIUS servers used for accounting are also used for authentication.
- The switch must be configured to access at least one RADIUS server.
- RADIUS servers are accessed in the order in which their IP addresses were configured in the switch. Use **show radius** to view the order. As long as the first server is accessible and responding to authentication requests from the switch, a second or third server will not be accessed.
- If access to a RADIUS server fails during a session, but after the client has been authenticated, the switch continues to assume the server is available to receive accounting data. Thus, if server access fails during a session, it will not receive accounting data transmitted from the switch.

Acct-Session-ID Options in a Management Session. The switch can be configured to support either of the following options for the accounting service types used in a management session. (Refer to "Accounting Service Types" on page 102.)

- unique Acct-Session-ID for each accounting service type used in the same management session (the default)
- same Acct-Session-ID for all accounting service types used in the same management session

Unique Acct-Session-ID Operation. In the Unique mode (the default), the various service types running in a management session operate as parallel, independent processes. Thus, during a specific management session, a given service type has the same Acct-Session-ID for all accounting actions for that service type. However, the Acct-Session-ID for each service type differs from the ID for the other types.

Note In Unique Acct-Session-ID operation, the Command service type is a special case in which the Acct-Session-ID for each executed CLI command in the session is different from the IDs for other service types used in the session *and also* different for each CLI command executed during the session. That is, the ID for each successive CLI command in the session is sequentially incremented from the ID value assigned to the immediately preceeding CLI command in that session.

- **Enhancement (PR_0000040783)** — This enhancement reduces the down time when unicast routing indicates a Candidate Rendezvous Point (C-RP) is not reachable. Upon detecting a C-RP has become unreachable, the Bootstrap Router (BSR) sends a new Bootstrap Message (BSM) with a zero holdtime for the unreachable C-RP. All devices in the PIM domain should then remove this C-RP from their RP-set.
- **Enhancement (PR_0000041395)** — Debug capability for PIM packet events is added. The command syntax is as follows.

```
ProCurveSwitch# debug ip pim packet
hello
register
join-prune
bsr
dr
rp
<cr>
```

Examples:

```
ProCurveSwitch# debug ip pim packet join
This command would show all prunes, joins, grafts, and graft-acks that are sent and received on the switch.
ProCurveSwitch# debug ip pim packet hello vlan 3,4,7-16
This command would show all hello packets sent and received on vlans 3, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16.
ProCurveSwitch# debug ip pim packet
Engages all pim packet debugging.
ProCurveSwitch# debug ip pim
Engages all pim debugging.
```

IP PIM debug output may be filtered further by specifying a source IP address, VLAN and group. Use the CLI help for syntax details.

Release K.14.47 Enhancements

Release K.14.47 includes the following enhancement.

- **Enhancement (0000041472)** — VRRP Ping Virtual IP of Backup.

VRRP Ping Virtual IP of Backup Overview

In many networks, edge devices are often configured to send packets to a statically configured default router. If this router becomes unavailable, the devices that use it as their first-hop router become isolated from the network. VRRP uses dynamic failover to ensure the availability of an end node's default router. This is done by assigning the IP address used as the default route to a "virtual router", or VR. The VR may include:

- an Owner router assigned to forward traffic designated for the virtual router (If the Owner is forwarding traffic for the VR, it is the Master router for that VR.)
- one or more prioritized Backup routers.

When in compliance with RFC 3768, only owner VRs reply to ping requests (ICMP echo requests) to the Virtual IP address (VIP). When this feature is enabled, a Backup VR operating as the Master can respond to ping requests made to the VIP. This makes it possible to test the availability of the default gateway with ping. A non-owner VR that is not master drops all packets to the VIP.

Note This feature is not a part of RFC 3768. Enabling this feature results in non-compliance with RFC 3768 rules.

Global Virtual IP Address Ping Control

The Backup router can be enabled to respond to pings using the following command.

Syntax: [no] router vrrp virtual-ip-ping

Enables or disables the response to a ping request for the switch. When enabled, all VRs that are not Owners and are not explicitly disabled (see **virtual-ip-ping enabled** *command) respond to ping requests sent to the VIP when the Backup VR is acting as Master.*

Default: Response to Virtual IP ping is disabled.

```
ProCurve-Router1# config
ProCurve-Router1(config)# ip routing
ProCurve-Router1(config)# router vrrp
ProCurve-Router1(config)# router vrrp virtual-ip-ping
```

Figure 75. Example of Enabling the Response to Ping Requests

Controlling Ping Responses

Use the following command to enable or disable responses to pings to a Virtual IP address. The command applies to all virtual IP addresses on the VR. It is executed in VR context and is available when the VR is configured as Backup.

Note This feature, which is a change in configuration, can only be enabled or disabled when the VR is disabled.

Syntax: [no] virtual-ip-ping enabled

Enables or disables the response to a ping request to a specific Virtual IP address.

Must be executed in VRRP context (vlan <vid> vrrp vrid <vrid>)

Note: The VR should be configured as a Backup.

Default: Enabled

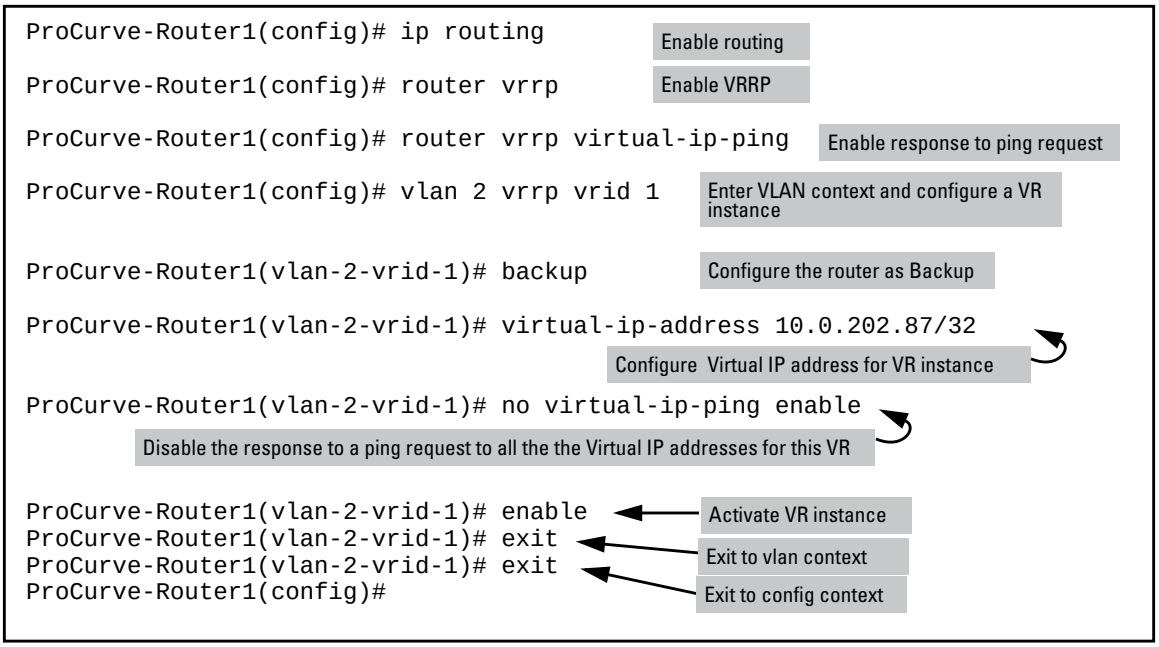


Figure 76. Example of Disabling a Response to Ping Requests to a Virtual IP Address

Displaying VRRP Ping Information

Display global VRRP configuration information by entering the **show vrrp config global** command.

```
ProCurve(config)# show vrrp config global
VRRP Global Configuration Information

 VRRP Enabled  : Yes
 Traps Enabled : Yes
 Virtual Routers Respond to Ping Requests [Yes] : Yes
```

Figure 77. Example of VRRP Global Configuration Information

Use the **show vrrp** command to display information about VRRP global statistics.

```
ProCurve(config)# show vrrp

 VRRP Global Statistics Information

  VRRP Enabled           : Yes
  Protocol Version       : 2
  Invalid VRID Pkts Rx   : 0
  Checksum Error Pkts Rx : 0
  Bad Version Pkts Rx    : 0
  Virtual Routers Respond To Ping Requests : Yes    Global VR ping information


 VRRP Virtual Router Statistics Information

  Vlan ID                  : 2
  Virtual Router ID        : 1
  State                    : Master
  Up Time                  : 25 secs
  Virtual MAC Address      : 00005e-000101
  Master's IP Address      : 10.0.102.87
  Associated IP Addr Count : 1          Near Failovers            : 0
  Advertise Pkts Rx        : 0          Become Master             : 1
  Zero Priority Rx         : 0          Zero Priority Tx          : 0
  Bad Length Pkts          : 0          Bad Type Pkts             : 0
  Mismatched Interval Pkts : 0          Mismatched Addr List Pkts : 0
  Mismatched IP TTL Pkts   : 0          Mismatched Auth Type Pkts : 0
```

Figure 78. An Example of VRRP Global Statistics Information

You can display VRRP configuration information using the **show vrrp config** command.

```
ProCurve-Router1(config)# show vrrp config

VRRP Global Configuration Information

VRRP Enabled  : Yes
Traps Enabled : Yes
Virtual Routers Respond to Ping Requests  : Yes    Global VR ping information

VRRP Virtual Router Configuration Information

Vlan ID : 2
Virtual Router ID : 1

Administrative Status [Disabled] : Enabled
Mode [Uninitialized] : Backup
Priority [100] : 150
Advertisement Interval [1] : 1
Preempt Mode [True] : True
Preempt delay time : 0
Respond to Virtual IP Ping Requests [Yes] : Yes
Primary IP Address : Lowest

IP Address      Subnet Mask
--------------- ---------------
10.0.202.87     255.255.0.0
```

Figure 79. Example of VRRP Configuration Display Showing Virtual IP Address Ping Status

Figure 80 displays the ping response status for a specific VLAN and VRID.

```
ProCurve-Router1(config)# show vrrp vlan 2 vrid 1 config

VRRP Virtual Router Configuration Information

Vlan ID : 2
Virtual Router ID : 1

Administrative Status [Disabled] : Enabled
Mode [Uninitialized] : Backup
Priority [100] : 150
Advertisement Interval [1] : 1
Preempt Mode [True] : True
Preempt delay time : 0
Respond to Virtual IP Ping Requests [Yes] : Yes
Primary IP Address : Lowest


IP Address      Subnet Mask
--------------- ---------------
10.0.202.87     255.255.0.0
```

Response to Ping Requests

Figure 80. Example of VRRP Configuration for a VLAN and VRID

The example in Figure 81 shows the gateway information for IP routes. A designation of “reject” means that the IP traffic for that route is discarded. For VIP entries, when the Backup ping feature is enabled, no ping error messages are sent for the discarded packets.

```
ProCurve(config)# show ip route


  Destination        Gateway         VLAN Type      Sub-Type   Metric     Dist.
  ------------------ --------------- ---- --------- ---------- ---------- -----
  10.0.0.0/16        DEFAULT_VLAN    1    connected            1          0
  10.0.202.87/32     reject               static               1          1
  127.0.0.0/8        reject               static               0          0
  127.0.0.1/32       lo0                  connected            1          0
```

Figure 81. Example of IP Route Information

Operational Notes

- Jumbo frames are supported if they have been enabled for that VLAN. The VIP responds to ping requests if they are not fragmented and are not larger than the Maximum Transmission Unit (MTU).
- Fragmented packets are not supported. All fragmented packets sent to a VIP are dropped and no response or error is sent.
- All packets with IP options are dropped. Any ping options will work as long as they do not change to IP options.
- ICMP requests other than echo requests are not supported.
- If there are errors in packets sent to a VIP, for example, “TTL Invalid”, no ICMP error packet is sent.
- **Enhancement (0000038652)** — Unauthenticated VLAN Access (Guest VLAN Access).

Unauthenticated VLAN Access Overview

When a PC is connected through an IP phone to a switch port that has been authorized using 802.1X or Web/MAC authentication, the IP phone is authenticated using client-based 802.1X or Web/MAC authentication and has access to secure, tagged VLANs on the port. If the PC is unauthenticated, it needs to have access to the insecure guest VLAN (unauthenticated VLAN) that has been configured for 802.1X or Web/MAC authentication. 802.1X and Web/MAC authentication normally do not allow authenticated clients (the phone) and unauthenticated clients (the PC) on the same port.

Mixed port access mode allows 802.1X and Web/MAC authenticated and unauthenticated clients on the same port when the guest VLAN is the same as the port's current untagged authenticated VLAN for authenticated clients, or when none of the authenticated clients are authorized on the untagged authenticated VLAN. Instead of having just one client per port, multiple clients can use the guest VLAN.

Authenticated clients always have precedence over guests (unauthenticated clients) if access to a client's untagged VLAN requires removal of a guest VLAN from the port. If an authenticated client becomes authorized on its untagged VLAN as the result of initial authentication or because of an untagged packet from the client, then all 802.1X or Web/MAC authenticated guests are removed from the port and the port becomes an untagged member of the client's untagged VLAN.

Characteristics of Mixed Port Access Mode

- The port keeps tagged VLAN assignments continuously.
- The port sends broadcast traffic from the VLANs even when there are only guests authorized on the port.
- Guests cannot be authorized on any tagged VLANs.
- Guests can use the same bandwidth, rate limits and QoS settings that may be assigned for authenticated clients on the port (via RADIUS attributes).
- When no authenticated clients are authorized on the untagged authenticated VLAN, the port becomes an untagged member of the guest VLAN for as long as no untagged packets are received from any authenticated clients on the port.
- New guest authorizations are not allowed on the port if at least one authenticated client is authorized on its untagged VLAN and the guest VLAN is not the same as the authenticated client's untagged VLAN.

Note If you disable mixed port access mode, this does not automatically remove guests that have already been authorized on a port where an authenticated client exists. New guests are not allowed after the change, but the existing authorized guests will still be authorized on the port until they are removed by a new authentication, an untagged authorization, a port state change, and so on.

Configuring Mixed Port Access Mode

Syntax: [no] aaa port-access <port-list> mixed

Enables or disables guests on ports with authenticated clients.

Default: Disabled; guests do not have access

```
ProCurve(config)# aaa port-access 6 mixed
```

Figure 82. Example of Configuring Mixed Port Access Mode

- **Enhancement (0000011015)** — Cached Reauthentication (Hold State if Radius Server Unavailable).

Cached Reauthentication Overview

Cached reauthentication allows 802.1X, web, or MAC reauthentications to succeed when the RADIUS server is unavailable. Users already authenticated retain their currently-assigned RADIUS attributes. Uninterrupted service is provided for authenticated users with RADIUS-assigned VLANS if the RADIUS server becomes temporarily unavailable during periodic reauthentications.

Cached reauthentication is similar to the authorized authentication method in that user credentials are not checked. Any user credentials are valid even if they are different from those used during the last successful authentication of the same session. However, cached reauthentication maintains the current session attributes, unlike the authorized authentication method. New authentications are not allowed. The RADIUS server can be the only allowed source of session attributes for authenticated users.

Reauthentications are not disabled when the RADIUS server is unavailable. The switch initiates reauthentications of clients at the specified period and the clients must comply with the requirements for the reauthentication procedure exactly as is done for the authorized authentication method.

The table below summarizes the differences between the authorized method and the cached reauthentication method.

Table 2. Summary of Cached Reauthentication and Authorized Authentication Characteristics

Authorized	Cached Reauthentication
New authentications are allowed when RADIUS server is unreachable.	New authentications are not allowed when RADIUS server is unreachable.
All previously RADIUS-assigned attributes are voided and replaced by switch-configured values on reauthentication when RADIUS server is unreachable.	All previously assigned attributes remain in effect on reauthentication when RADIUS server is unreachable.

Cached reauthentication is supported for 802.1X, Web authentication, and MAC authentication. For more information about Web/MAC authentication, see “Web and MAC Authentication” in the *Access Security Guide* for your switch. For more information on 802.1X, see “Configuring Port-Based and User-Based Access Control (802.1X) in the *Access Security Guide* for your switch.

Syntax: [no] aaa authentication <port-access | web-based | mac-based > <primary method> < secondary-method>

Allows reauthentications to succeed when the RADIUS server is unavailable. Users already authenticated retain their currently-assigned session attributes.

The primary methods for **port-access** *authentication are* **local**, **chap-radius**, *or* **eap-radius**.
The primary method for **web-based** *or* **mac-based** *authentication is* **chap-radius**.

The secondary methods can be **none**, **authorized**, *or* **cached-reauth**.

The default secondary authentication for all types of port access remains “none”.

Syntax: [no] aaa port-access <authenticator | web-based | mac-based> <***port-list***>
cached-reauth-period [1-2147483647]

Configures the period of time (in seconds) during which cached reauthentication is allowed on the port.

Default: No limit is set.

```
ProCurve(config)# aaa port-access web-based 6-8 cached-reauth-period 86400
```

The cached-reauth-period is set to 86400 **seconds** (1440 minutes, or 24 hours).

Figure 83. Example of Configuring the Maximum Number of Consecutive Cached Reauthentications

Timing Considerations

The reauth period when the RADIUS server is unavailable is the configured reauth period plus an additional *X* seconds, where *X* can vary from 1 to approximately 30 seconds in most cases, depending on the number of RADIUS servers and other RADIUS parameters. This period of time can be more or less than 30 seconds if the default "server-timeout" values for 802.1X or Web/MAC authentication have been changed from their default values. The period of time represented by *X* is how long 802.1X or Web MAC authentication will wait for a RADIUS response.

For example:

1. A cached-reauth-period is set to 900 seconds (15 minutes) and the reauth period is 180 seconds.
2. A client is successfully authenticated or reauthenticated.
3. The RADIUS server becomes unavailable. In 180 seconds from the authentication in step 1, 802.1X or Web/MAC authentication initiates reauthentication.
4. In *X* seconds after the initiation of authentication in step 3 (1 to 30 seconds if default values for 802.1X or Web/MAC authentication are used), 802.1x or Web/MAC authentication receives notification that the RADIUS server is unavailable.
5. 802.1X or Web/MAC authentication allows the first cached reauthentication and starts the cached reauth period.
6. A number of cached reauthentications occur within the 900 seconds after the start of the cached reauth period in step 5. These have a period of 180 + *X* seconds.
7. The cached reauthentication period (900 seconds) ends.
8. The next reauthentication begins 180 seconds after the last cached reauthentication.
9. In *X* seconds after the reauthentication in step 8, 802.1X or Web/MAC authentication receives notification that the RADIUS server is still unavailable.
10. 802.1X or Web/MAC authentication terminates the client's session.

Determining the Amount of Time Before Client Session Termination. 1.The maximum amount of time between step 2 and step 3 is 180 seconds.

2. The amount of time between step 3 and step 5 is *X* seconds.
3. The reauthentication in step 8 happens less than 180 seconds after step 7, and step 7 happens in 900 seconds after step 5. The maximum amount of time between step 5 and step 8 is 900 + 180 seconds.
4. The time between step 8 and step 9 is *X* seconds.
5. The total time is 180 + X + 900 + 180 + X, which equals 900 +2(180+X) seconds.

Note The period of 1 to 30 seconds, represented by *X*, is not a firm time period; the time can vary depending on other 802.1X and Web/MAC auth parameters.

Release K.14.48 Enhancements

Release K.14.48 includes the following enhancements. (Not a public release)

- **Enhancement (PR_0000016657)** — Access Control Debug Logging changes have been made.

Access Control Debug Logging

Debug logging provides real-time messages on the status of processes running on the switch. The access control changes deal mainly with the client authentication process.

The debug options include a new security branch that contains all the security features. The existing options are moved under a parent option of “security”. The new options also reside under the parent security option.

Existing Security Debug Options	New Security Debug Options
SSH	Radius
Dynamic Arp	Web-Auth (has subnodes)
Dsnoop agent events packets	Port Access authenticator (802.1X) mac-based supplicant (802.1X) web-based
Dynamic IP Lockdown	TACACS
	Port Security
	User Profile MIB

For more information about debug events, see “Using the Event Log for Troubleshooting Switch Problems” in the *Troubleshooting* chapter of the *Management and Configuration Guide* for your switch.

Syntax: debug security [arp-protect | dhcp-snooping | dynamic-ip-lockdown | port-access | port-security | radius-server | ssh | tacacs-server | user-profile-mib]

Displays debug messages for the selected option.

Default: Option is disabled.

```
ProCurve(config)# debug security ssh info
ProCurve(config)# debug security dhcp-snooping agent
ProCurve(config)# debug security port-access mac-based

ProCurve(config)# show debug

 Debug Logging

  Source IP Selection: Outgoing Interface
  Destination:    Session

Enabled debug types:
 security ssh (info)
 security dhcp-snooping agent
 security port-access mac-based
```

Figure 84. Example of Enabling Debug Messages for Selected Security Options

Events Logged

802.1X, Web/MAC, IDM, and DCA Authentication Debug Log Events

- A client authentication request is sent to RADIUS for a specific client on a port.
- A client authentication response is received from RADIUS for a specific client on a port.
- Access denied on a port because of conflicts with RADIUS-assigned attributes (VLAN).
- Displays RADIUS-assigned switch attributes for each user authenticated on the switch. VLAN attributes include tagged or untagged.
- Provides information on authentication process for a client, for example, client A detected on port B.
- Provides information about credentials obtained from a client if the client is rejected by the RADIUS server and placed on the Guest VLAN.
- Reauth timer information for Web Authentication.
- For Web Authentication, provides information on the protocols that are spoofed by Web Authentication (DHCP, DNS, ARP, EWA, redirect).
- When a client moves from one port to another, when enabled.
- When a client is deauthenticated due to reauth period, logoff period, or forced reauth.

Port Security Debug Log Events

- MAC addresses added through 802.1X or Web MAC authentication.
- MAC addresses that have been added, removed, learned, or aged on a port-security enabled port.

User Profile MIB Debug Log Events

- All clients that are added or removed from the user profile MIB through SNMP.

RADIUS and TACACS+ Debug Log Events

These debug log events cover management interface authentications (telnet, ssh, http, etc.) as well as access control authentication requests.

- Provides information about all RADIUS or TACACS+ request packets sent, for example, RADIUS request sent to server A for Client B on port 2.
- Provides information on all RADIUS or TACACS+ response packets received, for example, RADIUS response received on server A for Client B on port 2.

- All retries and timeouts for RADIUS or TACACS+ requests.
- All RADIUS drops due to bad attributes.

■ **Enhancement (PR_0000042147, PR_0000042840)** — Port-Based Debug Logging enhancement has been made.

Port-Based Debug Logging

■ This enhancement provides debug logging with the ability to filter debug messages related to a specific set of configured ports. When the port filter is enabled for a debug type, only the messages that inherently refer to a specific port will be filtered. All other messages for that debug type will still be sent to debug logging. The CLI command for this enhancement is below.

```
Switch# debug <security> <port-access | port-security | user-profile-mib> <optional
detailed debug type> include port [PORT-LIST]
```

The following is used to remove all ports:

```
Switch# [no] debug <security> <port-access | port-security |
user-profile-mib> <optional detailed debug type> include port
```

Release K.14.49 Enhancements

Software never built.

Release K.14.50 Enhancements

Release K.14.50 includes the following enhancement. (Not a public release)

■ **Enhancement (PR_0000048021)** — Support was added for the following products.

J9310A - HP ProCurve 3500yl-24G-PoE+ Switch
J9311A - HP ProCurve 3500yl-48G-PoE+ Switch
J9312A - HP ProCurve 10-GbE 2-Port SFP+/2-Port CX4 yl Module

Release K.14.54 Enhancements

Release K.14.54 includes the following enhancements. (Not a public release)

■ **Enhancement (PR_0000044183)** — Display interface configuration enhancement.

Display Configuration of Selected Interface

The options provided in this feature allow you to display all the configurations on a specified interface or VLAN with a single command. You can use the options with the startup config command, **show config**, and the running config command, **show running-config**.

Running Configuration Output

You can display the running configuration using this command. An example of the output is shown in Figure 85.

Syntax: show running-config [interface <port-list | loopback <0-7> | vlan <***vlan-id-list***>]

Displays running configuration information about the selected interface when one is specified. The interfaces can be ports, VLANs, or SVLANs.

Note Copying and pasting the displayed configuration information into the switch configuration is not supported. This feature only provides a display of all the configuration information for a selected interface or range of interfaces in a single view.

```
ProCurve(eth-A2-A4)# show running-config

Running configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "ProCurve Switch 5412zl"
interface A2
   disable
   name "test1"
   flow-control
   broadcast-limit 80
   speed-duplex 100-full
   unknown-vlans Block
   qos priority 4
   lacp Passive
   gvrp join-timer 30
   gvrp leave-timer 60
   gvrp leaveall-timer 700
exit
interface A3
   disable
   name "test1"
   flow-control
   broadcast-limit 80
   speed-duplex 100-full
   unknown-vlans Block
   qos priority 4
   lacp Passive
   gvrp join-timer 30
   gvrp leave-timer 60
   gvrp leaveall-timer 700
exit
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A4,C1-C24,F1-F24
   ip address dhcp-bootp
   exit
interface A2
   dhcp-snooping trust
   bandwidth-min output 20 10 10 10 20 10 10 10
   rate-limit bcast in percent 75
   ipv6 access-group "check" in
   exit
interface A3
   dhcp-snooping trust
   bandwidth-min output 20 10 10 10 20 10 10 10
   rate-limit bcast in percent 75
   ipv6 access-group "check" in
   exit
```

Configuration information for interfaces A2 and A3 is shown in two different places in the config file.

Figure 85. Example of Running Configuration Output for Interfaces A2 - A4

Figure 86 shows an example of the running config for a range of interfaces. The configuration information for interfaces A2 and A3 is now displayed together.

```
ProCurve(config)# show running-config interface A2-A3

Running configuration:

interface A2
   disable
   name "test1"
   flow-control
   broadcast-limit 80
   speed-duplex 100-full
   unknown-vlans block
   qos priority 4
   gvrp join-timer 30 leave-timer 60 leaveall-timer 700
   dhcp-snooping trust
   lacp passive
   bandwidth-min output 20 10 10 10 20 10 10 10
   rate-limit bcast in percent 75
   ipv6 access-group "check" in
   untagged vlan 1
   exit
interface A3
   disable
   name "test1"
   flow-control
   broadcast-limit 80
   speed-duplex 100-full
   unknown-vlans block
   qos priority 4
   gvrp join-timer 30 leave-timer 60 leaveall-timer 700
   dhcp-snooping trust
   lacp passive
   bandwidth-min output 20 10 10 10 20 10 10 10
   rate-limit bcast in percent 75
   ipv6 access-group "check" in
   untagged vlan 1
   exit
```

All the information for interfaces A2 and A3 is shown together in the output.

Figure 86. Example of Startup Config Output for a Specified Interface Range

Figure 87 shows an example of the running config file for a range of interfaces after some configuration changes have been made.

```
ProCurve(config)# no stack
ProCurve(config)# mesh 2-3
Command will take effect after saving configuration and reboot.

ProCurve(config)# write memory
ProCurve(config)# reload

ProCurve# show running-config interface 2-3

Running configuration:

interface 2
   untagged vlan 1
   mesh
   exit
interface 3
   flow-control
   untagged vlan 1
   mesh
   exit
```

Figure 87. Example of Running Config Output for a Range of Interfaces

Figure 88 is an example of the running config output showing VLAN information.

```
ProCurve(config)# show running-config

Running configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "ProCurve Switch 5412zl"
module 1 type J9309A
module 3 type J8702A
module 6 type J8702A
ip routing
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A4,C1-C24,F1-F24
   ip address dhcp-bootp
   exit
vlan 2
   name "test-vlan-2"
   ip helper-address 4.1.1.1
   ip helper-address 5.1.1.1
   ip address 1.1.1.1 255.255.255.0
   ipv6 address 2001::/64 anycast
   ipv6 enable
   exit
vlan 3
   name "VLAN3"
   ip helper-address 7.1.1.1
   ip forward-protocol udp 7.1.1.1 snmp
   ip forward-protocol udp 11.1.1.2 dns
   no ip address
   exit
vlan 4
   name "VLAN4"
   ip address 5.1.1.1 255.255.255.0
   ip bootp-gateway 5.1.1.1
   exit
logging 10.0.102.90
logging system-module ospf
ip route 5.1.1.0 255.255.255.0 vlan 4 distance 3
```

VLAN 4 configuration information is not together in the config file output.

Figure 88. Example of Running Config Output Showing VLAN Information

In Figure 89, the configuration information for VLAN 4 is now displayed in one place.

```
ProCurve(config)# show running-config vlan 3-4

Running configuration:

vlan 3
   name "VLAN3"
   ip helper-address 7.1.1.1
   ip forward-protocol udp 7.1.1.1 snmp
   ip forward-protocol udp 11.1.1.2 dns
   no ip address
   exit
vlan 4
   name "VLAN4"
   ip address 5.1.1.1 255.255.255.0
   ip bootp-gateway 5.1.1.1
   ip route 5.1.1.0 255.255.255.0 distance 3
   exit
```

VLAN 4 configuration information is displayed together in the output.

Figure 89. Example of Running Config Output for a Range of VLANs

Figure 90 shows an example of the running config for a range of VLANs after configuration changes have been made to selected VLANs.

```
ProCurve(config)# dhcp-snooping
ProCurve(config)# vlan 14
ProCurve(vlan-14)# exit
ProCurve(config)# vlan 15
ProCurve(vlan-15)# exit
ProCurve(config)# vlan 23
ProCurve(vlan-23)# exit
ProCurve(config)# dhcp-snooping vlan 14-15
ProCurve(config)# static-mac 00:11:22:33:44:55 vlan 23 interface A3
ProCurve(config)# spanning-tree instance 2 vlan 15

ProCurve(config)# show running-config vlan 14-15

Running configuration:

vlan 14
   name "VLAN14"
   no ip address
   dhcp-snooping
   exit
vlan 15
   name "VLAN15"
   no ip address
   dhcp-snooping
   spanning-tree instance 2
   exit
```

Figure 90. Example of Output for Running Config for a Range of VLANs

Startup Configuration Output

You can display the startup configuration using this command. An example of the startup configuration output is shown in Figure 91.

Syntax: show config [interface <port-list | loopback <0-7> | vlan <***vlan-id-list***>]

Displays startup configuration information about the selected interface when one is specified. The interfaces can be ports, VLANs, or SVLANs.

```
ProCurve(config)# show config

Startup configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "ProCurve Switch 5412zl"
module 1 type J9309A
module 3 type J8702A
module 6 type J8702A
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A4,C1-C9,C15-C24,F1-F24
   ip address dhcp-bootp
   no untagged C10-C14
   exit
vlan 5
   name "VLAN5"
   untagged C10-C14
   ip address 5.1.1.1 255.255.255.128
   exit
interface loopback 5
   ip address 7.1.1.1
   exit
interface loopback 7
   ip address 12.1.1.1
   exit
snmp-server community "public" unrestricted
```

Figure 91. Example of Startup Configuration Output

Figure 92 shows an example of the startup config output for a selected VLAN.

```
ProCurve(vlan-5)# show config vlan 5

Startup configuration:

vlan 5
   name "VLAN5"
   untagged C10-C14
   ip address 5.1.1.1 255.255.255.128
   exit
```

Figure 92. Example of Startup Config Output for a Specific VLAN

Figure 93 shows an example of the startup config output for a range of interfaces for a specific VLAN.

```
ProCurve(vlan-5)# show config interface C10-C13

Startup configuration:

interface C10
   untagged vlan 5
   exit
interface C11
   untagged vlan 5
   exit
interface C12
   untagged vlan 5
   exit
interface C13
   untagged vlan 5
   exit
```

Figure 93. Example of Startup Config Output for a Range of Interfaces for a Specific VLAN

- **Enhancement (PR_0000045649)** — Post-logon banner enhancement.

Post-Logon Banner

A text message that has been configured with the **banner motd** command displays with the authentication prompt when a user opens a console, telnet, SSH, or WebAgent session.

The **exec** option of the **banner** command allows a user-configurable message to be displayed after the user has been authenticated. If there is no password on the switch, the exec banner message displays immediately.

Syntax: [no] banner exec <***ASCII-string***>

Sets the exec banner text. Text can be multiple lines up to 3070 characters, and can consist of any printable character except the tilde (~) and the delimiting character.

<ASCII-string>*: The text must end with a delimiting character, which can be any single character except the tilde (~) character.*

The **no** *version of the command removes the banner exec text.*

```
ProCurve(config)# banner exec &
Enter TEXT message. End with the character &
This is Switch A in the language lab &
```

Figure 94. Example of the banner exec Command

To display the status and text for the exec banner configuration, use the **show banner exec** command.

```
ProCurve(config)# show banner exec

Banner Information

Banner Status: Enabled
Configured Banner:

This is Switch A in the language lab
```

Figure 95. Example Displaying Exec Banner Configuration

WebAgent Display of Exec Banner Message

If the MOTD banner message has been configured, it is displayed first. If the **exec** banner option has also been configured, the MOTD banner message is followed by a Continue link to the next page.

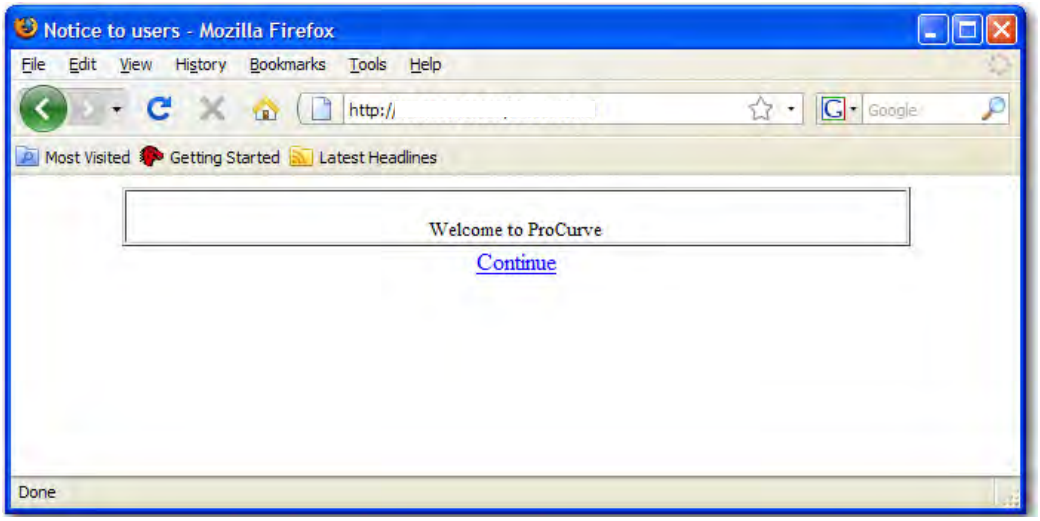


Figure 96. Example of MOTD Message in the WebAgent

Clicking on Continue displays the Username/Password dialog box if the switch has been configured with password security. If no password has been configured, the exec banner message displays immediately.

After being authenticated successfully when a password has been configured, the exec banner message displays. Click on the Continue link to proceed to the WebAgent Home Page.

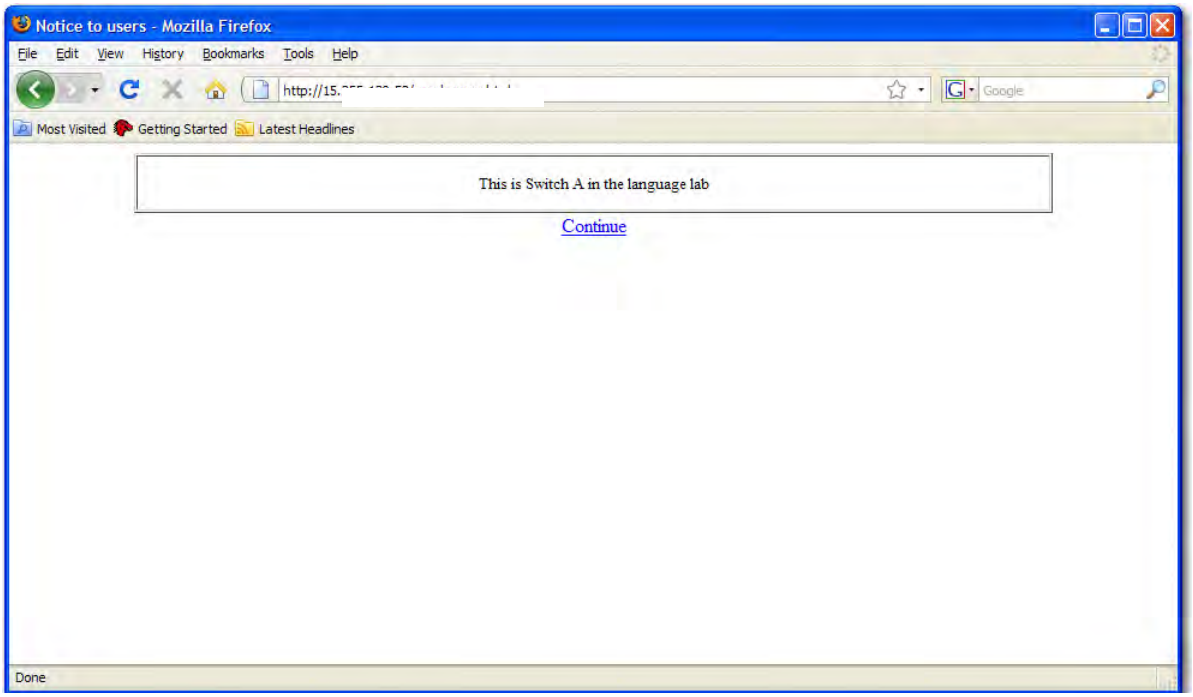


Figure 97. Example of Exec Banner Message

SNMP Support

The MIB variables required to support Exec banner are in the hpicfBasic.mib file.

Error Messages

Error Message	Description
Delimiter must be a single character	Use a single ASCII character for a delimiter at the end of the Exec Banner message
Tildes (~) are not allowed.	Do no use a tilde in the Exec Banner message.
String for Banner Exec is too long. Allowed length is 3070.	The Exec Banner message can be up to 3070 characters long.

- **Enhancement (PR_0000045711)** — Web authentication message enhancement.

Web Authentication Message

This feature allows administrators to configure custom messages that are displayed when authentication with the RADIUS server fails. The messages are appended to the existing internal web page that displays during the authentication process. Messages can be configured using the CLI, or centrally using the RADIUS server, and can provide a description of the reason for the failure as well as possible steps to take to resolve the authentication issue. There is no change to the current web authentication functionality..

Syntax: [no] aaa port-access web-based access-denied-message <<access-denied-str> | radius-response>

Specifies the text message (ASCII string) shown on the web page after an unsuccessful login attempt. The message must be enclosed in quotes.

The **no** *form of the command means that no message is displayed upon failure to authenticate.*

Default: The internal web page is used. No message will be displayed upon authentication failure.

access-denied-str*: The text message that is appended to the end of the web page when there is an unsuccessful authentication request. The string can be up to 250 ASCII characters.*

radius-response: *Use the text message provided in the RADIUS server response to the authentication request.*

```
ProCurve(config)# aaa port-access web-based access-denied-message “Please
contact your system administrator to obtain authentication privileges.”
```

Figure 98. Example of Configuring an Access Denied Message on the Switch

```
ProCurve(config)# show port-access web-based config

Port Access Web-based Configuration

DHCP Base Address     : 192.168.0.0
DHCP Subnet Mask      : 255.255.248.0
DHCP Lease Length     : 10 seconds
Allow RADIUS-assigned dynamic (GVRP) VLANs[No]: Yes
Access Denied Message : Custom:
  Please contact your system administrator to obtain authentication privileges.


     |         Client  Client  Logoff     Re-auth    Unauth   Auth    Ctrl
  Port | Enabled Limit   Moves   Period     Period     VLAN ID  VLAN ID Dir
  ---- + ------- ------- ------- ---------  ---------  -------  ------- -----
  A1   | Yes     1       No      300        60         1        2       both
  A2   | Yes     18      No      999999999  999999999  0        0       both
  A3   | Yes     22      No      999999999  999999999  4096     4096    both
```

Figure 99. Example of Output showing the Custom Access Denied Message

The example in Figure 100 shows the text of the Access Denied Message when the **radius-response** option is configured.

```
ProCurve(config)# show port-access web-based config

Port Access Web-based Configuration

DHCP Base Address     : 192.168.0.0
DHCP Subnet Mask      : 255.255.248.0
DHCP Lease Length     : 10 seconds
Allow RADIUS-assigned dynamic (GVRP) VLANs[No]: Yes
Access Denied Message : Retrieved from Radius


      |         Client  Client  Logoff     Re-auth    Unauth  Auth    Ctrl
  Port | Enabled Limit   Moves   Period     Period     VLAN ID VLAN ID Dir
  ---- + ------- ------- ------- ---------  ---------  ------- ------- -----
  A1   | Yes     1       No      300        60         1       2       both
  A2   | Yes     18      No      300        999999999 0       0       both
  A3   | Yes     22      No      300        999999999 4096    4096    both
```

Figure 100. Example of Access Denied Message when radius-response is Configured

Unauthenticated clients may be assigned to a specific static, untagged VLAN (**unauth-vid**), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients, the port is blocked and no network access is available.

Web Page Display of Access Denied Message

The web page in Figure 101 is an example of the denied access message that appears when **unauth-vid** is configured.

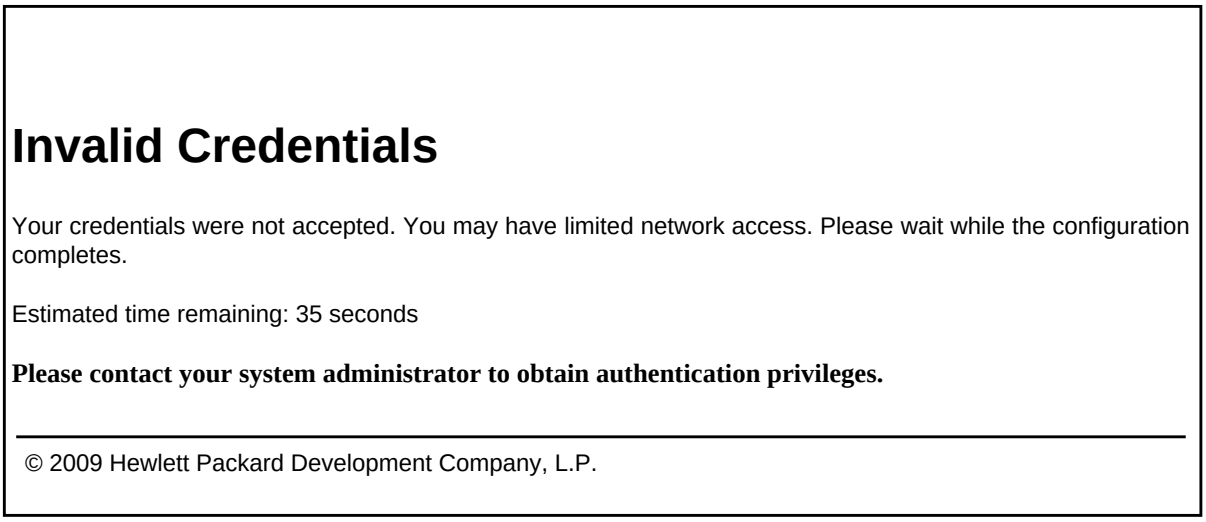


Figure 101. Example of Web Page with Configured Access Denied Message When unauth-vid is Configured

Figure 102 shows an example of a web page displaying the access denied message when un **auth-vid** is not configured.

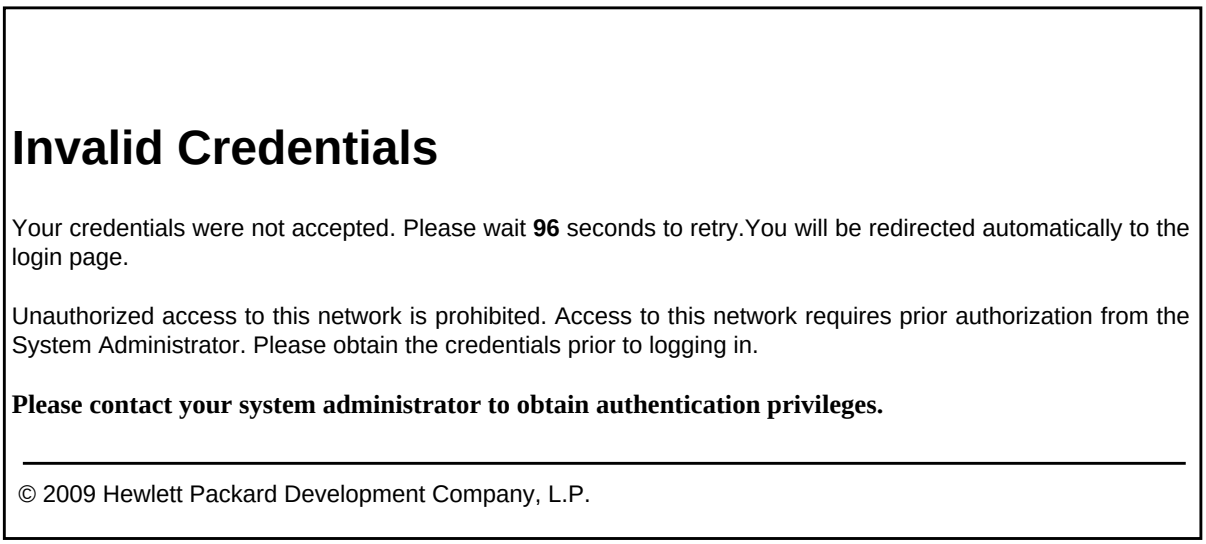


Figure 102. Example of Web Page with Configured Access Denied Message When unauth-vid is not Configured

The **show running-config** command displays the client's information, including the configured access denied message.

```
ProCurve(config)# show running-config

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "ProCurve Switch 3500yl-24G"
web-management ssl
qos dscp-map 000000 priority 0
module 1 type J86xxA
module 3 type J8694A
no stack auto-join
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-14,19-24,A1-A4
   ip address dhcp-bootp
   no untagged 15-18
   exit
vlan 100
   name "auth-vid"
   untagged 15-18
   ip address dhcp-bootp
   exit
radius-server host 10.0.13.118 key 'secret'
aaa authentication port-access eap-radius
snmp-server community "public" Unrestricted
aaa port-access web-based 5
aaa port-access web-based 5 auth-vid 100
aaa port-access web-based 5 unauth-vid 1
aaa port-access web-based dhcp-addr 172.18.0.0 255.255.255.0
aaa port-access web-based access-denied-message “Please contact your system
administrator to obtain authentication privileges.”
no autorun
```

Access denied message

Figure 103. Example of Running Configuration Output Displaying Access Denied Message

```
ProCurve(config)# show running-config

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "ProCurve Switch 3500yl-24G"
web-management ssl
qos dscp-map 000000 priority 0
module 1 type J86xxA
module 3 type J8694A
no stack auto-join
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-14,19-24,A1-A4
   ip address dhcp-bootp
   no untagged 15-18
   exit
vlan 100
   name "auth-vid"
   untagged 15-18
   ip address dhcp-bootp
   exit
radius-server host 10.0.13.118 key 'secret'
aaa authentication port-access eap-radius
snmp-server community "public" Unrestricted
aaa port-access web-based 5
aaa port-access web-based 5 auth-vid 100
aaa port-access web-based 5 unauth-vid 1
aaa port-access web-based dhcp-addr 172.18.0.0 255.255.255.0
aaa port-access web-based access-denied-message radius-response
```

RADIUS response configured

Figure 104. Example of Running Configuration Output When RADIUS Response is Configured

- **Enhancement (PR_0000045749)** — Module reload enhancement.

Module Reload

The Module reload feature allows you to reset a module by initiating a warm reboot of a specified module or modules. This saves time over rebooting the entire switch, which can take several minutes to complete and disrupts all users on the switch. The specified module has its power turned off, and then turned on again. This causes the module to reset to a known good state and reload its software.

Syntax: [no] reload [[after < [[DD:] HH:] MM>] | [at HH:MM [:SS] [MM/DD[/[YY]YY]]] |
[module <***slot-id range***>]]

When specified with the **module** *parameter, initiates a reload of the module in the specified slot or slots by turning the slot power off, then on again. A valid slot or range of slots must be specified. The* **at** *and* **after** *parameters are not allowed with the* **module** *option. The* **no** *version of the command is not valid with the* **module** *option.*

When the **reload** *command is executed without any parameters, an immediate switch reload occurs.*

Note: This feature is not supported for ProCurve One modules.

at: *Schedules a whole switch reload at a specified date and time. The time must not be more than 99 days in the future. Minimum required input is* **HH:MM**. *Cannot be used with the* **module** *option.*

after: *Schedules a whole switch reload after the specified length of time, which must not be more than 99 days in the future. Minimum required input is* **MM**. *Cannot be used with the* **module** *option*

module: *Powers the module on or off, forcing a software reload of the specified module or modules.*

```
ProCurve(config)# reload module C
The ‘reload module’ command will shutdown the specified modules. Ports on specified
modules will no longer pass traffic. Any management traffic to the switch which
passes through the affected modules will be interrupted (e.g. ssh, telnet, snmp).
This command may take up to 2 minutes to power down all specified modules. Please
check the event log for current status of module power down, power up cycle. Continue
[y/n]?
```

Figure 105. Example of Reloading a Specified Module

Use the **show reload** command to display the reload information. This can include:

- A scheduled, pending reload of the entire switch
- A statement that no reload is scheduled
- The time of the last reload of each module on the system

```
ProCurve(config)# reload at 23:45
Reload scheduled at 23:45:47 6/16/2010
(in 0 days, 1 hours, 41 minutes)

ProCurve(config)# show reload at
Reload scheduled for 23:45:47 06/16/2010
(in 0 days, 1 hours, 40 minutes)

ProCurve(config)# show reload after
Reload scheduled for 23:45:47 6/16/2010
(in 0 days, 1 hours, 40 minutes)
```

Figure 106. Example of the Scheduled Reload At Information

```
ProCurve(config)# reload after 35
Reload scheduled in 0 days, 0 hours, 35 minutes


ProCurve(config)# show reload at
Reload scheduled in 0 days, 0 hours, 34 minutes

ProCurve(config)# show reload after
Reload scheduled in 0 days, 0 hours, 34 minutes
```

Figure 107. Example of the Scheduled Reload After Information

```
ProCurve(config)# show reload module

Module Reload information:

Module | Last reload date
-------+----------------------
  C      10:50:51 01/13/2010
```

Figure 108. Example of the Module Reload Information

- **Enhancement (PR_0000045752)** — User-configurable per-port MAC address enhancement.

User-Configurable Per-Port MAC Address

User-configurable per-port MAC addresses have been limited to 32 addresses. This enhancement increases the number of user-configurable per-port MAC addresses from 32 to 64 addresses. The switch-wide per-port address limit is unchanged.

Release K.14.55 Enhancements

Release K.14.55 includes the following enhancement. (Not a public release)

- **Enhancement (PR_0000018427)** — Multicast ARP support enhancement.

Multicast ARP Support

To support IP multicasting, the multicast address range of 01-00-5E-00-00-00 to 01-00-5E-7F-FF-FF is reserved for Ethernet MAC addresses. The command **ip arp-mcast-replies** enables acceptance of the MAC addresses in the IP multicast range.

Syntax: [no] ip arp-mcast-replies

Enables or disables accepting multicast MAC addresses in the IP multicast address range in ARP requests and replies.

Default: Disabled.

```
ProCurve(config)# ip arp-mcast-replies
```

Figure 109. Example of Enabling the Acceptance of Multicast MACs in the IP Multicast Range

Release K.14.59 Enhancements

Release K.14.59 includes the following enhancements. (Not a public release)

- **Enhancement (PR_0000018479)** — Longer usernames and passwords are now allowed, and some special characters may be used.

Username and Password Size Increase

For security reasons, it is desirable to allow the configuration of longer usernames and passwords than is currently allowed on the switch. The limits on length will be extended to 64 characters for the following authentication methods:

- Front-end—WEB User Interface, SSH, and Telnet
- Back-end—RADIUS, TACACS+, and Local

General Rules for Usernames and Passwords

Usernames and passwords are case-sensitive. ASCII characters in the range of 33-126 are valid, including:

- A through Z uppercase characters
- a through z lower case characters
- 0 through 9 numeric characters
- Special characters ‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ‘ “ , < > / ? (see Restrictions, below)

The SPACE character is allowed to form a username or password pass-phrase. The username must be in quotes, for example **“The little brown fox”**. A space is not allowed as part of a username without the quotes. A password that includes a space or spaces should not have quotes.

Restrictions for the Setmib Command

Usernames and passwords can be set using the CLI command **setmib**. They cannot be set using SNMP.

- Quotes are permitted for enclosing other characters, for example, a username or password of **abcd** can be enclosed in quotes **“abcd”** without the quotes becoming part of the username or password itself. Quotes can also be inserted between other characters of a username or password, for example, **ab”cd**. A pair of quotes enclosing characters followed by any additional characters is invalid, for example, **“abc”d.**
- Spaces are allowed in usernames and passwords. The username or password must be enclosed in quotes, for example, **“one two three”.** A blank space or spaces between quotes is allowed, for example, **“ ”**.

Additional Restrictions

Some authentication servers prevent the usage of special symbols such as the backslash (\) and quotes (“”). ProCurve allows the use of these symbols in configurable credentials, but using them may limit access for some users who may use different client software. Please refer to the vendor’s documentation for specific information about these restrictions.

Operating Notes on Upgrading or Downgrading Software Versions

Upgrading from K.14.pre-release to K.14.release Software

When you upgrade to software version K.14.release from a prior software version, the existing usernames and passwords continue to be there; no further action is required.

Downgrading from K.14.release Software or Installing K.15.01 Software

If you install a prior software version (K.14.pre-release and below) that does not support the increase in length and the use of special characters for the username/password, or if you install the K.15.01 software version, you must do one of the following:

1. Reset the username and/or password to be no more than 16 characters in length, and without any special characters, using the CLI command **password** or the equivalent in the WebAgent. If the include-credentials feature is enabled or was previously enabled, execute a CLI **write memory** command.

```
ProCurve(config)# password manager
New password: ********
Please retype new password: *******

ProCurve(config)# write mem
```

Or

2. Execute the CLI command **no password all.** This clears all the passwords.If the include-credentials feature is enabled or was previously enabled, execute a CLI **write memory** command.

```
ProCurve(config)# no password all
Password protections will be deleted, do you want to continue [y/n]? y
ProCurve(config)# write mem
```

Or

3. Clear all of the configuration by executing the CLI command **erase startup config.** This removes the *entire* configuration and immediately reboots the switch.

```
ProCurve(config)# erase startup config
Configuration will be deleted and device rebooted, continue [y/n]? y
```

If the include-credentials feature has not been enabled, then perform either step 1 or step 2. If the include-credentials feature has been enabled, perform steps 1, 2, or 3.

Not Supported—Software Version K.15.01 Downgrade to K.14.release

A downgrade from software version K.15.01 to K.14.release is not supported. The username will be lost. You must set the username again after booting the K.14.release software image. However, the password is preserved and you will see a password prompt.

If You Cannot Access the Switch

If you cannot access the switch after a software version downgrade, perform one of the following steps to recover access.

1. If the include-credentials feature is enabled, boot the software image and perform steps 1, 2, or 3 in the preceding section.

Or

2. If the include-credentials feature is not enabled, boot the software image and perform steps 1 or 2 in the preceding section.

Or

3. Boot the software image and press the **Clear** button on the front of the switch. This resets the passwords. You can use this regardless of whether the include-credentials feature is enabled or disabled.

- **Enhancement (PR_0000045707)** — The tilde character is now allowed in TACACS+ and RADIUS encryption keys.

Support for the Tilde (~) Character in TACACS+ and RADIUS Keys

This feature allows you to configure a TACACS+ or RADIUS encryption key that includes a tilde (~) as part of the key, for example, "hp~procurve". It is not backward compatible; the "~" character is lost if you use a software version that does not support the "~" character.

SNMP already supports the inclusion of the tilde character in a key.

Configuring TACACS+ Keys

Global Keys

If you need only one encryption key for the switch to use in all attempts to authenticate through a TACACS+ server, configure a global key.

To configure a global encryption key for TACACS+, enter this command.

Syntax: [no] tacacs-server key <***key-string***>

Configures an optional global encryption key. Keys configured in the switch must exactly match the encryption keys configured in the TACACS+ servers that the switch will attempt to use for authentication.

The **no** *form of the command removes the global encryption key.*

```
ProCurve(config)# tacacs-server key hp~procurve

ProCurve(config)# show tacacs
Status and Counters - TACACS Information
Timeout: 5
Source IP Selection: Outgoing Interface
Encryption Key: hp~procurve

Server IP Addr Opens Closes Aborts Errors Pkts Rx Pkts Tx OOBM
-------------- ----- ------ ------ ------ ------- ------- ----
10.10.10.2     0     0      0      0      0       0       0
```

Figure 110. Example of Configuring a Global Encryption Key for TACACS+ with a ~ Character

Host-Specific Keys

If the switch is configured to access multiple TACACS+ servers having different encryption keys, you can configure the switch to use different encryption keys for different TACACS+ servers.

Syntax: [no] tacacs-server host <***ip-addr***> [key <***key-string***>]

Adds a TACACS+ server and optionally assigns a server-specific encryption key.

The **no** *form of the command removes a TACACS+ server assignment (including its server-specific encryption key, if any).*

```
ProCurve(config)# tacacs-server host 10.10.10.2 key hp~procurve
```

Figure 111. Example of Configuring a Host-Specific Key

Use the **show running-config** command to display the key information.

```
ProCurve(config)# show running-config

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "ProCurve Switch 3500yl-24G"
module 1 type J86xxA
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address dhcp-bootp
   exit
banner motd "good morning
tacacs-server host 10.10.10.2 key "hp~procurve"
snmp-server community "public" unrestricted
```

Shows the key configured for a specific host.

Figure 112. Example of the Running Configuration File Showing the Host-Specific Key for TACACS+ with the "~" Included

For more information about TACACS+, see the chapter 'TACACS+ Authentication" in the *Access Security Guide* for your switch.

Configuring RADIUS Keys

Global Keys

To configure a global key for RADIUS authentication, enter this command.

Syntax: [no] radius-server key <***global-key-string***>

Specifies the global encryption key the switch uses with servers for which the switch does not have a server-specific key assignment. This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key.

Default: Null

The **no** *form of the command removes the global encryption key.*

```
ProCurve(config)# radius-server key hp~procurve

ProCurve(config)# show radius
Status and Counters - General RADIUS Information
Deadtime (min): 0
Timeout: 5
Retransmit Attempts: 3
Global Encryption Key: hp~procurve
Dynamic Authorization UDP Port: 3799
Source IP Selection: Outgoing Interface

          Auth Acct DM/Time

Server IP Addr Port Port CoA Window Encryption Key OOBM
-------------- ---- ---- --- ------ -------------- ----
10.33.18.127   1812 1813 No  300                    No
```

Global encryption key

Figure 113. Example of RADIUS Global Encryption Key with a ~ Character Included

Host-Specific Keys

To configure a host-specific key for RADIUS authentication, enter this command.

Syntax: [no] radius-server host <***ip-address***> key <***key-string***>

Optional. Specifies an encryption key for use during authentication (or accounting) sessions with the specified server. This key must match the encryption key used on the RADIUS server. Use this command only if the specified server requires a different encryption key than configured for the global encryption key.

Default: Null

Use the **no** *form of the command to remove the key for a specified server.*

```
ProCurve(config)# radius-server host 10.33.18.127 key hp~procurve

ProCurve(config)# show radius

  Status and Counters - General RADIUS Information

   Deadtime(min) : 0
   Timeout(secs) : 5
   Retransmit Attempts : 5
   Global Encryption Key :

                   Auth   Acct
  Server IP Addr   Port   Port  Encryption Key
  --------------   ----   ----- --------------------
  10.33.18.127     1812   1813  hp~procurve
```

Figure 114. Example of Host-Specific Key for RADIUS Authentication

```
ProCurve(config)# show running

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "ProCurve Switch 3500yl-24G"
module 1 type J86xxA
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address dhcp-bootp
   exit
banner motd "good morning
radius-server host 10.33.18.127 key "hp~procurve"
snmp-server community "public" unrestricted
```

Shows the key configured for a specific host.

Figure 115. Example of Running Configuration File Showing the Host-Specific Key for RADIUS Authentication

For more information about RADIUS keys, see the chapter "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide* for your switch.

- **Enhancement (PR_0000052732)** — Enhancement to increase the MAC Authentication Client Limit to 256.

Increase MAC Auth Client Limit to 256

The client limit is 256 clients per-port for MAC-auth and Web-auth; the client limit for 802.1X is 32 clients per port. The MAC-auth and Web-auth limit of 256 clients only applies when there are fewer than 16,384 authentication clients on the entire switch. After the limit of 16, 384 clients is reached, no additional authentication clients are allowed on any port for any method.

The following commands are used to specify client limits:

```
aaa port-access mac-based <port-list> [addr-limit]
aaa port-access web-based <port-list> [client-limit]
aaa port-access authenticator <port-list> [client-limit]
```

- **Enhancement (PR_0000052801)** — Categorize CLI Return Messages enhancement.

Categorize CLI Return Messages

When a CLI command returns a message, that message is now prefixed with a category describing the type, as follows:

- Error
- Warning
- Information

Syntax: session show-message-type [enable | disable]

When enabled, the CLI return messages are prefixed with string that indicates the type of message. Entered at the manager level.

The **disable** *option disables prefixing returned messages for the session for which this command is executed.*

Note: This setting is not saved when the switch is rebooted.

Default: Disabled on all CLI sessions

```
ProCurve(config)# router rip
Error: IP Routing support must be enabled first.

ProCurve(config)# qinq mixed vlan
Warning: This command will reboot the device. Any prior configuration on this
config file will be erased and the device will boot up with a default configuration
for the new qinq mode.
Do you want to continue [y/n]? n

ProCurve(config)# snmp-server mib hpSwitchAuthMIB included
Information: For security reasons, network administrators are encouraged to
disable SNMPv2 before using the MIB.
```

Figure 116. Examples of Message Prefixes

To determine if message labeling is enabled, enter the **show session** command.

```
ProCurve(config)# show session
Show Message Type: Enabled
CLI Interactive Mode: Enabled
```

Figure 117. Example Showing the label cli-return-message Command is Enabled

CLI Interactive Commands

When the CLI interactive command mode is enabled, you must explicitly enter the choice of yes (**y**) or no (**n)** for interactive commands. When interactive command mode is disabled, the default choice for all command is **yes**, except as noted below. The CLI interactive mode command enables or disables interactive mode for the CLI session.

Syntax: session interactive-mode [enable | disable]

Enables or disables interactive mode for the CLI session.

The **disable** *option disables interactive mode. The default choice for yes/no interactive commands will be* **yes** *except for commands when there is a prompt to save the config. The default for that is* **no**.

The default choice for rebooting the switch is **yes**.

Note: This setting is not saved when the switch is rebooted.

Default: Enabled on all sessions.

```
ProCurve(config)# no password all
Password protection for all will be deleted, continue [y/n]? y
```

Default choice is **yes**.

```
ProCurve(config)# boot system flash secondary
System will be rebooted from secondary image. Do you want to continue [y/n]? y
Do you want to save current configuration [y/n]? n
```

Default choice for reboot is **yes**. Default choice for saving the current configuration is **no**.

Figure 118. Example of CLI Interactive Mode When Disabled

To determine if the CLI interactive mode is enabled or disabled, enter the **show session** command.

```
ProCurve(config)# show session
Show Message Type: Enabled
CLI Interactive Mode: Enabled
```

Figure 119. Example Showing CLI Interactive Mode is Enabled

Interactive Commands Requiring Additional Options

Interactive commands that require input other than yes or no are not affected when CLI interactive mode is disabled. A warning message is displayed when these commands are executed, for example:

```
Interactive mode is disabled; This command will be ignored. Enable
cli-interactive-mode to use this command.
```

The following commands will issue this warning when interactive mode is disabled. An alternate way to enter the command (when one is available) is shown.

Command	Non-Interactive Alternate Command
setup mgmt-interfaces	No equivalent non-interactive command
aaa port-access supplicant <port-list> secret	aaa port-access supplicant <port-list> secret <secret-string>
password manager	password manager plaintext <password-string>
password operator	password operator plaintext <password-string>

Command	Non-Interactive Alternate Command
aaa port-access supplicant <port-list> secret	aaa port-access supplicant <port-list> secret <secret-string>
crypto host-cert generate self-signed	crypto host-cert generate self-signed <start-date> <end-date> <CNAME-STR> <ORG-UNIT-STR> <ORGANIZATION-STR> <CITY-STR> <STATE-STR> <code>

Menu Commands

When CLI interactive mode is disabled, all CLI commands that launch the menu interface will not be affected by the interactive mode. A warning message is displayed, for example:

```
ProCurve(config)# menu
Interactive mode is disabled; This command will be ignored. Enable
cli-interactive-mode to use this command.
```

Other menu-based commands that will not be affected are:

- setup
- show interfaces display

SNMPv3 Special Cases

The following are special cases when using SNMPv3 with interactive mode.

- **snmpv3 user**: In interactive mode, the command **snmpv3 user** will create snmpv3 users, even if snmpv3 has not been enabled.
- **snmpv3 enable:** When interactive mode is disabled, this command only enables snmpv3. It does not prompt for an authentication password. When the command is first executed, a default initial user is created. A message displays:

  ```
  User ‘initial’ has been created.
  ```

Banner MOTD Command with Non-Interactive Mode

The use of escape characters allows the **banner motd** command to be used in non-interactive mode for multiple message lines. In non-interactive mode, you can create a banner message enclosed in double quotes or other delimiter that uses escape characters within the delimiters. Other existing CLI commands do not support the escape characters.

The following escape characters are supported:

\”	double q
\’	single quote
\`	forward quote
\\	backslash
\f	form feed
\n	newline
\r	carriage return
\t	horizontal tab
\v	vertical tab

```
ProCurve(config)# banner motd "You can use the \’banner motd\’ CLI command in
non-interactive mode.\n\n\tThe banner motd command will support escape charac-
ters."

ProCurve(config)# show banner motd

Banner Information

Banner status: Enabled

Configured Banner:

You can use the ‘banner motd’ CLI command in non-interactive mode.

     The banner motd command will support escape characters.”
```

Figure 120. Example of Configuring the Banner Message Using Escape Characters Within Double Quote Delimiters

The running configuration file contains the banner message as entered in the command line.

```
ProCurve(config)# show running-config

Running configuration:

;J8693A Configuration Editor; Created on release #K.14.00x

hostname “ProCurve”
vlan 1
  name “DEFAULT_VLAN”
  untagged 1-48, a1-a4
  ip address dhcp-bootp
  exit
banner motd “You can use the \’banner motd\’ CLI command in non-interactive
mode.\n\n\tThe banner motd command will support escape characters."
```

Figure 121. Example of the Running Config File with Banner MOTD Configured in Non-interactive Mode

You can use a delimiting character other than quotes as well, as shown in Figure 122.

```
ProCurve(config)# banner motd #
Ehter TEXT message. End with the character ‘#’
You can use the \’banner motd\’ CLI command in non-interactive mode.\n\n\tThe
banner motd command will support escape characters.#
```

Figure 122. Example of Configuring the Banner Message Using an Alternate Delimiter of ‘#’

Release K.14.62 Enhancements

Show MAC with VLAN

Enhancement (PR_0000052738) — Adds VLAN information to the output of the **show mac-address** commands.

This feature displays the VLAN ID with each MAC address for the **show mac-address <option>** command.

```
ProCurve(config)# show mac-address 4-6


 Status and Counters - Port Address Table - 4

  MAC Address   VLAN
  ------------- ----
  001186-f47ff4 2

 Status and Counters - Port Address Table - 5

  MAC Address   VLAN
  ------------- ----
  001279-7fbaf4 4

 Status and Counters - Port Address Table - 6

  MAC Address   VLAN
  ------------- ----
  001321-1763ca 4
```

Figure 123. Example of Output for show mac-address <port-list> Command

```
ProCurve(config)# show mac-address 001635-36de76

 Status and Counters - Address Table - 001635-36de76

 Port  VLAN
 ----- ----
 7     5
```

Figure 124. Example of Output for show mac-address <mac-address> Command

```
ProCurve(config)# show mac-address vlan 5

 Status and Counters - Address Table - VLAN 5

 MAC Address   Port
 ------------- ----
 001635-36de76 7
```

Figure 125. Example of Output for show mac-address vlan <vid> Command

```
ProCurve(config)# show mac-address

 Status and Counters - Port Address Table

 MAC Address   Port  VLAN
 ------------- ----  ----
 001635-36de76 7     1
 00934f-894rd2 5     1
 098745-de4928 6     1
```

Figure 126. Example of Output showing Ports and VLAN IDs for all MAC Addresses

Block Unknown Multicast

Enhancement (PR_0000053047) — Adds a global configuration option that allows each VLAN to have a multicast filter.

This feature adds a global IGMP multicast configuration option to the switch that results in each VLAN having a multicast filter. The filter prevents unjoined multicast traffic from being forwarded on interfaces associated with IGMP queriers. Each filter only contains interfaces that are queriers on the same VLAN, so multicast traffic is only flooded on interfaces that contain queriers that are on the same VLAN as the multicast traffic.

On switch bootup, all VLANs that are IGMP-enabled are guaranteed one multicast filter. You can always reboot the switch to recreate this configuration where each IGMP-enabled VLAN has a multicast filter.

Note Joined multicast traffic continues to be forwarded as usual.

It is necessary to reboot the switch after configuring the per-VLAN filter.

Syntax: [no] igmp filter-unknown-mcast

Enables interface isolation for unjoined multicast groups. IGMP is configured so that each interface with IGMP enabled will have a data-driven multicast filter associated with it, preventing unjoined IP multicast packets from being flooded. A reboot is required for the change to take effect.

Default: Disabled

```
ProCurve(config)# igmp filter-unknown-mcast
Command will take effect after saving configuration and reboot.
```

Figure 127. Example of Enabling the IGMP Multicast Filter

The following example shows the multicast traffic being flooded to all queriers on all VLANs; this is the default behavior. The **igmp filter-unknown-mcast** command has not been executed.

Table 3. Multicast Filter Table on Distribution Switch

VLAN ID	Member Ports
0 (all VLANs)	1, 2, 3

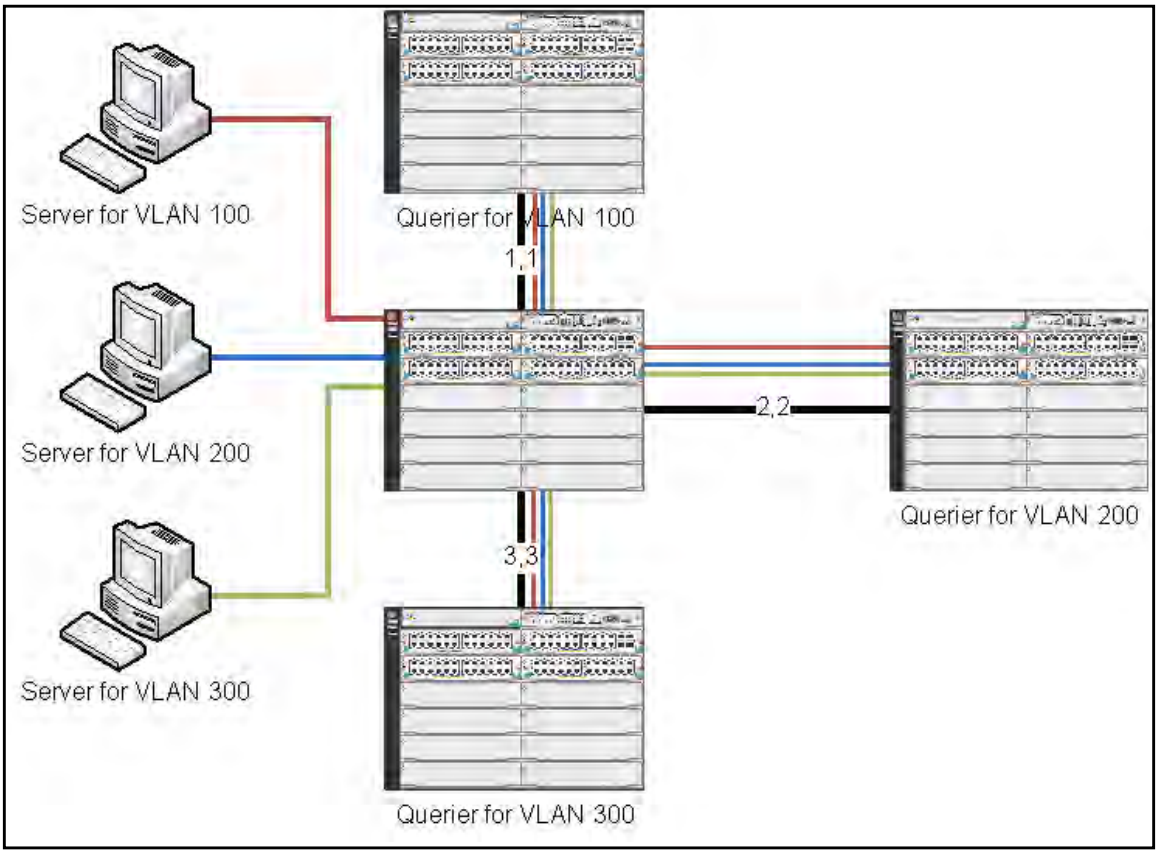


Figure 128. Example of Unknown Multicast Traffic Flooding on All Ports Connected to a Querier for Any VLAN

In the example shown in Figure 129, **igmp filter-unknown-mcast** has been configured. The multicast traffic only goes to the querier on the same VLAN as the multicast server.

Table 4. Multicast Filter Table on Distribution Switch

VLAN ID	Member Ports
100	1
200	2
300	3

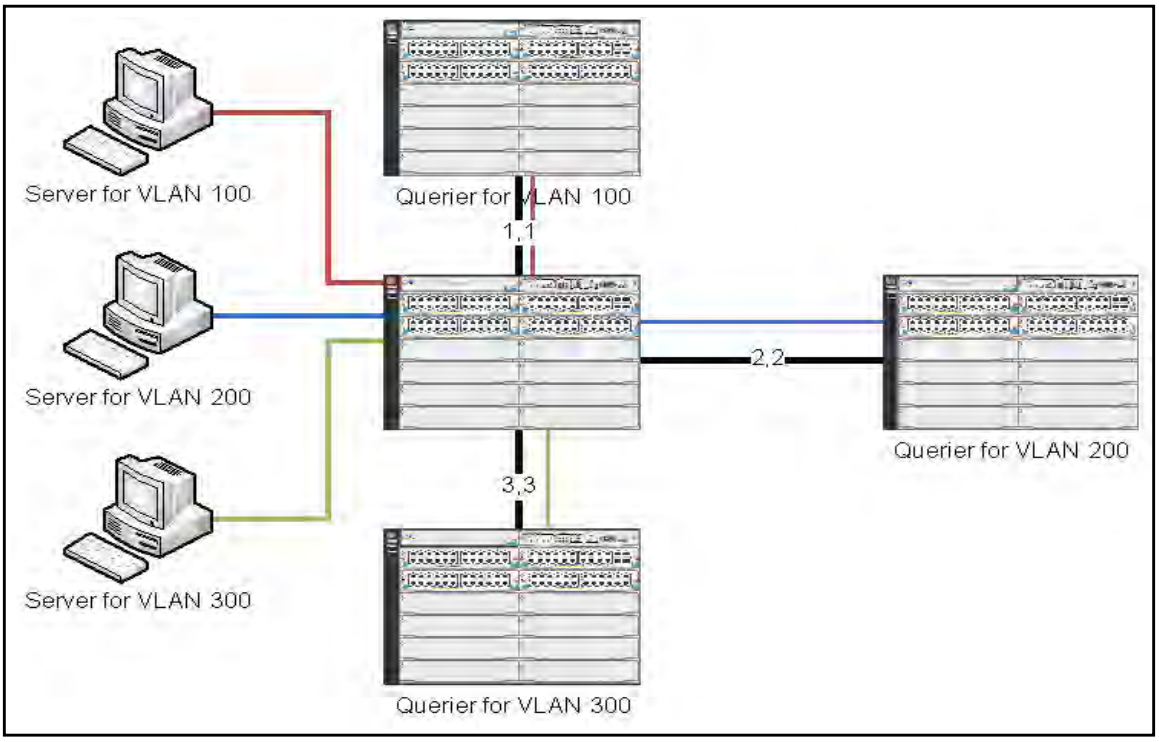


Figure 129. Example of Unknown Multicast Traffic Not Flooding out Ports Connected to Queriers in Separate VLANs

To display the status of IGMP multicast filtering use the **show ip igmp** command. If the IGMP Filter Unknown Multicast setting is different from the IGMP Filter Unknown Multicast status, a reboot is required to activate the desired setting. This setting will then be reflected in the status.

```
ProCurve(config)# show igmp filter-unknown-multicast

 IGMP Filter Unknown Multicast: Enabled
 IGMP Filter Unknown Multicast Status: Disabled
```

IGMP Filter Unknown Multicast setting

IGMP Filter Unknown Multicast status

If the IGMP Filter Unknown Multicast setting is different from the IGMP Filter Unknown Multicast Status, a reboot is required to activate the desired setting. This setting will then be reflected in the status.

Figure 130. Example of IGMP Unknown Multicast Filter Setting Being Enabled, but not yet Activated.

To display information about IGMP multicast filtering by interface, use the **show ip igmp** command.

```
ProCurve(config)# show ip igmp

Status and Counters - IP Multicast (IGMP) Status

IGMP Filter Unknown Multicast: Enabled
IGMP Filter Unknown Multicast Status: Enabled

 VLAN ID: 1
 VLAN Name : DEFAULT_VLAN
  IGMP is enabled

 VLAN ID : 100
 VLAN Name : VLAN100
  IGMP is enabled

 VLAN ID : 200
 VLAN Name : VLAN200
  IGMP is enabled

 VLAN ID : 300
 VLAN Name : VLAN300
  IGMP is enabled
```

Figure 131. Example of Output Displaying the Status of IGMP Unknown Multicast Filtering

MIB Information

The MIB object information is shown below.

```
    hpicfIgmpFilterUnknownMulticast OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION "Enable interface isolation for unjoined multicast groups.
                     Configures IGMP so that each interface with IGMP enabled
                     will have a data driven multicast filter associated with
                     it, preventing unjoined IP Multicast packets from being
                     flooded.  A reboot is required for this change to take
                     effect. The default is false/disabled(2)"
        DEFVAL      {false}
        ::= { hpicfIgmp 10 }

    hpicfIgmpFilterUnknownMulticastStatus OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The operational status of the IGMP Filter Unknown
                     Multicast mode. A value of true indicates the
                     hpicfIgmpFilterUnknownMulticast setting is
                     operational.  A value of false indicates the
                     hpicfIgmpFilterUnknownMulticast setting is not
                     operational.  A user action such as a reboot
                     may be necessary for the device to use the
                     hpicfIgmpFilterUnknownMulticast setting."
        DEFVAL      {false}
        ::= { hpicfIgmp 11 }
```

Outbound Queue Monitor

Enhancement (PR_0000054042)— Adds the ability to monitor egress queues for dropped packets when QoS is configured.

When QoS is used to prioritize traffic, different kinds of traffic can be assigned to different egress queues. If there is a great deal of traffic, it is desirable to be able determine if some traffic to the lower priority queues was dropped. This feature allows the egress queues for one port to be monitored for dropped packets.

Syntax: [no] qos watch-queue <port> out

Configures the switch to start monitoring the specified port for the dropped packets for each queue. Disabling and then re-enabling monitoring on a port clears the per-queue dropped packet counters.

The **no** *form of the command stops the collection of dropped traffic information.*

Default: Disabled

```
ProCurve(config)# qos watch-queue 5 out
```

Figure 132. Example of Configuring Monitoring for Dropped Packets

Displaying Per-Queue Counts

The **show interface queues** command displays the number of dropped packets for each queue for the configured port. The port must have been configured with the **qos watch-queue** command. Ports that have not been configured display zero values for the queue counts.

```
ProCurve(config)# show interface queues 5

Status and Counters - Queue Counters for port 5

  Name  :
  MAC Address      : 001c2e-95ab3f
  Link Status      : Up
  Port Totals (Since boot or last clear) :
   Rx Ucast Pkts   : 142,181              Tx Ucast Pkts   : 552
   Rx B/Mcast Pkts : 10,721,488           Tx B/Mcast Pkts : 11,765
   Rx Bytes        : 1,267,216,218        Tx Bytes        : 2,652,372
   Rx Drop Packets : 0                    Tx Drop Packets : 0
  Egress Queue Totals (Since boot or last clear) :
   Queue CoS  Dropped Packets
   1     1-2  123456789012345
   2     0,3  12345678
   3     4-5  1234
   4     6-7  0
```

Figure 133. Example of Monitoring Egress Queues on a Port

Show OSPF Neighbor Timers

Enhancement (PR_0000054055) — This enhancement provides the ability to display OSPF neighbor timer information.

This enhancement provides the ability to display the OSPF neighbor timer information by adding the **detail** option to the **show ip ospf neighbor** command.

Syntax: show ip ospf neighbor [detail [router-id]]

The detail option displays the OSPF neighbor timer information. You can optionally enter the router-id of the neighbor for which detail information is wanted.

There are two new counters that display neighbor timer information:

- Dead-timer Expires (HH:MM:SS): The time remaining for an active adjacency to expire if there are no more hello packets received.
- Neighbor Uptime (HH:MM:SS): The amount of time an adjacency is active.

If a neighbor loses adjacency and then re-establishes it, the Neighbor Uptime counter is set to zero. The Dead-timer Expires counter is set to the dead interval for the interface.

If a graceful restart of the neighbor occurs, the Neighbor Uptime counter continues to increment as the adjacency is considered active while the neighbor is restarting. The Dead-timer Expires counter is set to the hold timer for the neighbor. When the restart completes, the counter is set to the dead interval for the interface.

```
ProCurve(config)# show ip ospf neighbor detail

OSPF Neighbor Information for neighbor 10.10.10.2

IP Address: 10.10.10.2
Router ID : 10.10.10.2      State                     : FULL
Interface : vlan-10         Designated Router         : 10.10.10.3
Area      : backbone        Backup Designated Router  : 10.10.10.2
Priority  : 1               Retransmit Queue Length   : 0
Options   : 0               Neighbor Uptime           : 0h:0m:32s
Events    : 6               Dead Timer Expires        : 32 sec
```

Figure 134. Example of Displaying OSPF Neighbor Timers

IP Enable/Disable for All VLANs

Enhancement (PR_0000054183)—The user can now disable the IP addresses on specified VLANs, without deleting the configured IP addresses.

This enhancement allows you to administratively disable the IP address on specified VLANs with static IP addresses without removing the Layer 3 configuration. The switch can be pre-configured as a backup router, then quickly transition from backup to active by re-enabling Layer 3 routing on one or more VLANs. While the switch is in “backup” mode, it will still performing Layer 2 switching.

A MIB object will be toggled to make Layer 3 routing active or inactive on a VLAN.

Interaction with Other Features

The feature affects management access to the switch as follows:

- IP—SNMP, Telnet, SSH, HTTP, TFTP, SCP, SFTP
- Routing—RIP, OSPF, PIM, VRRP

When the **disable layer3** command is configured on a VLAN, the behavior is as if no IP address were configured for that VLAN. There is no other change in behavior.

Syntax: [no] disable layer3 vlan <vid | range of vids>

In config context, turns off Layer 3 routing for the specified VLAN or VLANs. When executed in vlan context, turns off Layer 3 routing for that VLAN.

The **no** *form turns on Layer 3 routing for the specified VLAN or VLANs.*

If QinQ is enabled, **svlan** *can be configured as well.*

The **show ip** command displays "disabled" in the IP Config column if Layer 3 has been disabled, or if the VLAN has no IP configuration. You can tell which is the case by viewing the remaining columns; if there is no IP configuration, the remaining columns are blank.

```
ProCurve(config)# show ip

 Internet (IP) Service

  IP Routing : Disabled

  Default Gateway : 172.22.16.1
  Default TTL     : 64
  Arp Age         : 20
  Domain Suffix   :
  DNS server      :

  VLAN                | IP Config  IP Address      Subnet Mask     Proxy ARP
  ------------------- + ---------- --------------- --------------- ---------
  DEFAULT_VLAN        | DHCP/Bootp 172.22.18.100   255.255.248.0   No No
  VLAN3               | Disabled   172.17.17.17    255.255.255.0   No No
  VLAN6               | Disabled
  VLAN7               | Manual     10.7.7.1        255.255.255.0   No No
```

Figure 135. Example of VLAN Disabled for Layer 3

For IPv6, the “Layer 3 Status” field displays the status of Layer 3 on that VLAN.

```
ProCurve(config)# show ipv6

 Internet (IPv6) Service

  IPv6 Routing    : Disabled
  Default Gateway :
  ND DAD          : Enabled
  DAD Attempts    : 3

  Vlan Name       : DEFAULT_VLAN
  IPv6 Status     : Disabled
  Layer 3 Status  : Enabled

  Vlan Name       : layer3_off_vlan
  IPv6 Status     : Disabled
  Layer 3 Status  : Disabled

  Address    |                                          Address
  Origin     | IPv6 Address/Prefix Length               Status
---------- + ---------------------------------------- -----------
  manual     | abcd::1234/32                            tentative
  autoconfig | fe80::218:71ff:febd:ee00/64              tentative
```

Figure 136. Example of IPv6 Layer 3 Status for a VLAN

Interactions with DHCP

Disabling Layer 3 functionality and DHCP are mutually exclusive, with DHCP taking precedence over **disable layer3** on a VLAN. The following interactions occur:

- If the **disable layer3** command is executed when DHCP is already configured, no disabling of the VLAN occurs. This error message displays —“Layer 3 cannot be disabled on a VLAN that has DHCP enabled.”
- From the CLI: If **disable layer3** is configured already, and an attempt is made to configure DHCP, DHCP takes precedence and will be set. The warning message displays— “Layer 3 has also been enabled on this VLAN since it is required for DHCP.”
- From the CLI: When disabling a range of VLAN IDs, this warning message displays— “Layer 3 will not be disabled for any LANs that have DHCP enabled.”
- From SNMP: If the disable layer3 command is executed when DHCP is already configured, no disabling of the VLAN occurs. An INCONSISTENT_VALUE error is returned.
- From SNMP: If disable layer3 is configured already, and an attempt is made to configure DHCP, DHCP takes precedence and will be set.

Release K.14.63 Enhancements

Enhancement (PR_0000040979) — The entry-count parameter is added to these two commands: **show access-list** and **show policy**. When either of those commands is used with the entry-count parameter, the switch displays the number of configured class, policy, and ACL entries.

Release K.14.65 Enhancements

LLDP PoE+ Enhancements

Enhancement (PR_0000046912)— Adds support for LLDP-PoE+ .

Overview

The data link layer classification (DLC) for PoE provides more exact control over the power requirement between a PSE and PD. The DLC works in conjunction with the physical layer classification (PLC) and is mandatory for any Type-2 PD that requires more than 12.95 watts of input power.

Note DLC is defined as part of the IEEE 802.3at standard.

The power negotiation between a PSE and a PD can be implemented at the physical layer or at the data link layer. After the link is powered at the physical layer, the PSE can use LLDP to repeatedly query the PD to discover the power needs of the PD. Communication over the data link layer allows finer control of power allotment, which makes it possible for the PSE to supply dynamically the power levels needed by the PD. Using LLDP is optional for the PSE but mandatory for a Type 2 PD that requires more than 12.95 watts of power.

If the power needed by the PD is not available, that port is shut off.

PoE Allocation

There are two ways LLDP can negotiate power with a PD:

- Using LLDP MED TLVs: Disabled by default. Can be enabled using the **int <*port-list*> PoE-lldp-detect [enabled | disabled]** command, as shown below. LLDP MED TLVs sent by the PD are only used to negotiate power if the LLDP PoE+ TLV is disabled or inactive; if the LLDP PoE+ TLV is sent as well (not likely), the LLDP MED TLV is ignored.
- Using LLDP PoE+ TLVs: Enabled by default. The LLDP PoE+ TLV is always advertised unless it has been disabled. It is enabled using the **lldp config <*port-list*> dot3TlvEnable poeplus_config** command. See "Enabling Advertisement of PoE+ TLVs" on page 148 for the command syntax.) It always takes precedence over the LLDP MED TLV.

Enabling **PoE-lldp-detect** allows the data link layer to be used for power negotiation.When a PD requests power on a PoE port, LLDP interacts with PoE to see if there is enough power to fulfill the request. Power is set at the level requested. If the PD goes into power-saving mode, the power supplied is reduced; if the need for power increases, the amount supplied is increased. PoE and LLDP interact to meet the current power demands.

Syntax: int <***port-list***> PoE-lldp-detect [enabled | disabled]

Allows the data link layer to be used for power negotiation between a PD on a PoE port and LLDP. Default: Disabled

For example, you can enter this command to enable LLDP detection:

```
ProCurve(config)# int 7 PoE-lldp-detect enabled
```

or in interface context:

```
ProCurve(eth-7)# PoE-lldp-detect enabled
```

Note Detecting PoE information via LLDP only affects power delivery; it does not affect normal Ethernet connectivity.

You can view the settings by entering the **show power-over-ethernet brief** command:

```
HPswitch(config)# show power-over-ethernet brief

Status and Counters - Port Power Status

  System Power Status    : No redundancy
  PoE Power Status       : No redundancy

  Available: 300 W  Used: 0 W  Remaining: 300 W

  Module A Power
  Available: 300 W  Used: 5 W  Remaining: 295 W

  PoE    | Power  Power    Alloc Alloc Actual Configured  Detection   Power
  Port   | Enable Priority By    Power Power  Type        Status      Class
  ------ + ------ -------- ----- ----- ------ ----------- ----------- -----
  A1     | Yes    low      usage 17 W  5.0 W  Phone1      Delivering  1
  A2     | Yes    low      usage 17 W  0.0 W              Searching   0
  A3     | Yes    low      usage 17 W  0.0 W              Searching   0
  A4     | Yes    low      usage 17 W  0.0 W              Searching   0
  A5     | Yes    low      usage 17 W  0.0 W              Searching   0
  A6     | Yes    low      usage 17 W  0.0 W              Searching   0
```

Figure 137. Example of Port with LLDP Configuration Information Obtained from the Device

Enabling Advertisement of PoE+ TLVs

To initiate the advertisement of power with PoE+ TLVs, the following command is configured with the **poeplus_config** option.

Syntax: lldp config <port-list> dot3TlvEnable poeplus_config

Enables advertisement of data link layer power using PoE+ TLVs.The TLV is processed only after the physical layer and the data link layer are enabled. The TLV informs the PSE about the actual power required by the device.

Default: Enabled

Displaying PoE When Using LLDP Information

To display information about LLDP port configuration, use the **show lldp config** command.

Syntax: show lldp config <port-list>

Displays the LLDP port configuration information, including the TLVs advertised.

```
HPSwitch(config)# show lldp config 4

 LLDP Port Configuration Detail

  Port : 4
  AdminStatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False


  TLVS Advertised:
   * port_descr
   * system_name
   * system_descr
   * system_cap

   * capabilities
   * network_policy
   * location_id
   * poe

   * macphy_config
   * poeplus_config

  IpAddress Advertised:
```

Figure 138. Example of LLDP Port Configuration Information with PoE

Figure 139 shows an example of the local device power information using the **show lldp info local-device <*port-list*>** command.

```
HPswitch(config) show lldp info local-device A1

LLDP Local Port Information Detail

  Port     : A1
  PortType : local
  PortId   : 1
  PortDesc : A1
  Pvid     : 1

Poe Plus Information Detail

    Poe Device Type            : Type2 PSE
    Power Source               : Primary
    Power Priority             : low
    PD Requested Power Value   : 20 Watts
    PSE Actual Power Value     : 20 Watts
```

Figure 139. Example of Local Device Power Information

Figure 140 shows an example of the remote device power information using the **show lldp info remote-device <*port-list*>** command.

```
HPswitch(config) show lldp info remote-device A3

LLDP Remote Device Information Detail

  Local Port   : A3
  ChassisType  : mac-address
  ChassisId    : 00 16 35 ff 2d 40
  PortType     : local
  PortId       : 23
  SysName      : HPswitch
  System Descr : HP Switch 3500-24, revision K.14.65
  PortDescr    : 23
  Pvid         : 55

  System Capabilities Supported  : bridge, router
  System Capabilities Enabled    : bridge

  Remote Management Address
     Type    : ipv4
     Address : 10.0.102.198


  Poe Plus Information Detail

    Poe Device Type            : Type2 PD
    Power Source               : Only PSE
    Power Priority             : low
    PD Requested Power Value   : 20 Watts
    PSE Actual Power Value     : 20 Watts
```

Figure 140. Example of Remote Device Power Information

See the chapter "Power over Ethernet (PoE/PoE+) Operation" in the *Management and Configuration Guide* for your switch for more information about PoE.

Console Local—Terminal None

Enhancement (PR_0000054059)— Adds the ability to configure the **console local-terminal** settings without entering config mode.

This enhancement allows you to use the console local-terminal command available in manager mode and operator mode as well as config mode. The configuration does not persist across a reboot.

Syntax: [no] console local-terminal <vt100 | ansi | none>

Set type of terminal being used for the current console or telnet session (default is vt100).

```
ProCurve# console local-terminal   <-- Console local-terminal command in manager mode.

ProCurve> console local-terminal   <-- Console local-terminal command in operator mode.
```

Figure 141. Example of console local-terminal Command in Manager and Operator Modes

Release K.14.67

Log Message When Startup Config Updated

- Enhancement (PR_0000052266) - Adds the ability to enable an SNMP trap when the switch's startup configuration is changed.

This enhancement enables notification to a management station when changes to the startup configuration file occur and are written to flash. Changes to the configuration file can occur when executing a CLI **write** command, executing an SNMP **set** command directly using SNMP, or when using the WebAgent.

A log message is always generated when a change occurs. An example log entry is:

```
I 07/06/10 18:21:39 02617 mgr: Startup configuration changed by SNMP. New seq. number 8
```

The corresponding trap message is sent if the **snmp-server enable traps startup-config-change** command is configured.

Syntax: [no] snmp-server enable traps startup-config-change

Enables notification of a change to the startup configuration. The change event is logged.

Default: Disabled

An example of configuring the command with the CLI is shown in Figure 142. The number that displays when **show config** is executed is global for the switch and represents the startup configuration sequence number.

```
ProCurve(config)# snmp-server enable traps startup-config-change

ProCurve(config)# show config

Startup configuration: 16

; J8697A Configuration Editor; Created on release #K.14.54

hostname “ProCurve Switch”
module 1 type J8702A
vlan 1
   name “DEFAULT_VLAN”
   untagged A1-A24, B1-B10
   ip address dhcp-bootp
   exit
snmp-server community “public” unrestricted
```

The number “**16**” is global for the switch and represents the startup configuration sequence number.

Figure 142. Example of Enabling Notification of Changes to the Startup Config File

Figure 143 displays an example o f the fields in the trap when a change is made via SNMP (station ip=0xAC161251 (172.22.18.81), no username is set, and the new sequence number is 16).

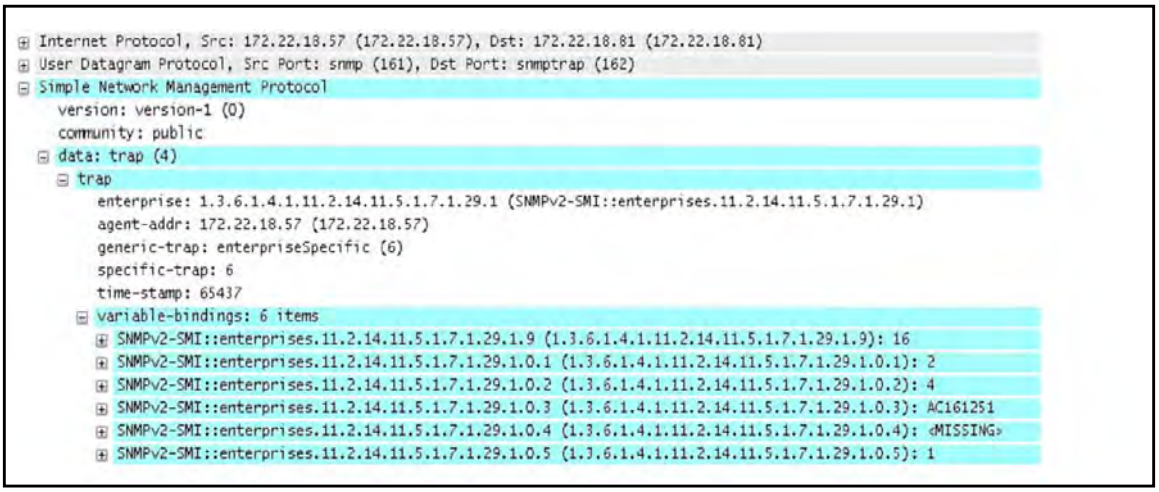


Figure 143. Example of the Fields When the SNMP Trap is Set

Release K.14.70

Logging for Routing ACLs

- Enhancement (PR_0000055367) - Adds the ability to log ACL “permit” entries.

This feature will provide functionality for logging ACL “permit” entries in the same manner that ACL “deny” entries are currently logged.

Operating Notes

- Affects only ACLs that are statically configured using the CLI command interface.
- Existing ACL logging for “deny” entries does not change
- A detailed event will be logged for the first packet that matches a “permit” or “deny” ACL logged entry with the appropriate action specified.
- Subsequent packets matching ACL logged entries will generate a new event that summarizes the number of packets that matched each specific entry (with the time period), for example:

  ```
  Mar 1 10:01:01 10.10.20.1 ACL:
  ACL 03/01/10 10:01:01: ACL NO-TELNET seq#10 permitted 6 packets
  ```

- Events are logged as specified by the **debug <destination>** command.
- Events are only logged when ACL logging is enabled using the **debug acl** command. This feature should only be used to troubleshoot and verify ACL configurations as it can impact switch performance even when ACL debugging is disabled.

Standard ACLs

The following abbreviated syntax is for standard, named ACLs. See the chapter “IPv4 Access Control Lists (ACLs)” in the *Access Security Guide* for your switch for more information on ACLs and ACL syntax.

Syntax: ip access-list standard < ***name-str*** >

*Places the CLI in the "Named ACL" (***nacl***) context specified by the < **name-str** > alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.*
< *name-str* >: *Specifies an identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: "***Accounting ACL***".*

< deny | permit >
< any | host < ***SA*** > | ***SA*** <mask | ***SA/ mask-length*** >> [log]

Executing this command appends the ACE to the end of the list of ACEs in the current ACL. In the default ACL configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.

SA=Source Address

Note: To insert a new ACE between two existing ACEs, precede **deny** *or* **permit** *with an appropriate sequence number.*

< deny | permit >

*For named ACLs, used in the "Named ACL" (***nacl***) context to configure an ACE. Specifies whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.*

[log]

This option generates an ACL log message if:

- *There is a match.*
- *ACL logging is enabled on the switch.*

(Use the debug command to direct ACL logging output to the current console session and/or to a Syslog server. Note that you must also use the **logging < *ip-addr* >** *command to specify the addresses of Syslog servers to which you want log messages sent.*

```
ProCurve(config)# ip access-list standard Sample-List
ProCurve(config-std-nacl)# permit host 10.10.10.104 log
ProCurve(config-std-nacl)# deny 10.10.10.1/24 log
ProCurve(config-std-nacl)# permit any
ProCurve(config-std-nacl)# exit
ProCurve(config)# _
```

Logging is configured for "permit" and "deny" ACEs.

Figure 144. Example of Standard ACL showing the log Option configured for both "permit" and "deny" ACEs

Extended ACLs

The following abbreviated syntax is for extended, named ACLs. See the chapter "IPv4 Access Control Lists (ACLs)" in the *Access Security Guide* for your switch for more information on ACLs and ACL syntax.

Syntax: ip access-list extended < ***name-str*** >

*Places the CLI in the "Named ACL" (***nacl***) context specified by the <* ***name-str*** *> alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.*
< name-str >: *Specifies an alphanumeric identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: "***Accounting ACL***". You can also use this command to access an existing, numbered ACL.*

Syntax: (nacl context) < deny | permit > < ip | ***ip-protocol*** | ***ip-protocol-nbr*** >
< any | host < ***SA*** > | ***SA/ mask-length*** | ***SA < mask >*** >
< any | host < ***DA*** > | ***DA/ mask-length*** | ***DA < mask >*** >
[precedence] [tos] [log]

Appends an ACE to the end of the list of ACEs in the current ACL. In the default configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.

SA=Source Address
DA=Destination Address

Note: To insert a new ACE between two existing ACEs in an extended, named ACL, precede **deny** *or* **permit** *with an appropriate sequence number along with the ACE keywords and variables you want.*

For a match to occur, a packet must have the source and destination addressing criteria specified in the ACE, as well as:

- *the protocol-specific criteria configured in the ACE, including any included, optional elements (described later in this section)*
- *any (optional) precedence and/or ToS settings configured in the ACE.*

< deny | permit >

*For named ACLs, these keywords are used in the "Named ACL" (***nacl***) context to specify whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.*

[log]

This option can be used after the DA to generate an Event Log message if:

- *There is a match.*
- *ACL logging is enabled.*

```
ProCurve(config)# ip access-list extended Extended-List-01
ProCurve(config-ext-nacl)# permit tcp host 10.10.10.44 host
10.10.20.78 eq telnet
ProCurve(config-ext-nacl)# deny ip 10.10.10.1/24 10.10.20.1/24
ProCurve(config-ext-nacl)# permit ip 10.10.10.2/24 log
ProCurve(config-ext-nacl)# exit
ProCurve(config)# vlan 10 ip access-group Extended-List in
```

Logging is configured for "permit" ACE.

Figure 145. Example of Standard ACL showing the log Option configured for a "permit" ACE

IPv6 Access Lists

The following abbreviated syntax is for IPv6, named ACLs. See the chapter "IPv6 Access Control Lists (ACLs)" in the *IPv6 Configuration Guide* for your switch for more details about IPv6 ACLs.

Syntax: ipv6 access-list < ***ascii-str*** >

*Places the CLI in the IPv6 ACL (***ipv6-acl***) context specified by the <* ***ascii-str*** *> alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.*
< ascii-str >: *Specifies an alphanumeric identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: "***Accounting ACL***". You can also use this command to access an existing ACL.*

Syntax: (ipv6 acl context) < deny | permit > < ipv6 | ***ipv6-protocol*** | ***ipv6-protocol-nbr*** >
< any | host < ***SA*** > | ***SA/prefix-length*** >
< any | host < ***DA*** > | ***DA/prefix-length*** >
[dscp < ***tos-bits*** | ***precedence***] [log]

Appends an ACE to the end of the list of ACEs in the current ACL. In the default configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.

SA=Source Address
DA=Destination Address

Note: To insert a new ACE between two existing ACEs in an ACL, precede **deny** *or* **permit** *with an appropriate sequence number.*

For a match to occur, a packet must have the source and destination IPv6 addressing criteria specified in the ACE, as well as:

- *the protocol-specific criteria configured in the ACE, including any optional elements (described later in this section)*
- *any (optional) DSCP settings configured in the ACE*

< deny | permit >

*These keywords are used in the IPv6 (***ipv6-acl***) context to specify whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.*

[log]

This option can be used after the DA to generate an Event Log message if:

- *There is a match.*
- *ACL logging is enabled.*

For a given ACE, if **log** is used, it must be the last keyword entered.

```
Port-1(config)# show access-list config

ipv6 access-list "Test-01"
     10 permit ipv6 2001:db8::1:10:10/128 ::/0 log
     20 deny tcp 2001:db8::1:20:0/121 2001:db8::1:10:3/128 eq 23 log
     30 deny ipv6 2001:db8::1:20:0/121 2001:db8::1:10:4/128 log
     40 deny tcp 2001:db8::1:30:0/121 2001:db8::1:10:4/128 eq 23 log
     50 deny ipv6 2001:db8::1:30:0/121 2001:db8::1:10:3/128
     60 deny icmp ::/0 ::/0 133
     70 permit ipv6 ::/0 ::/0
   exit
```

Logging is configured for "permit" and "deny" ACEs.

Figure 146. Example of Standard ACL showing the log Option configured for "permit" and "deny" ACEs

Release K.14.75

Copy command-file

- **Enhancement (PR_0000063482)** - The **copy command-file** feature now works for configuration commands other than ACLs.

Software Fixes

Software fixes are listed in chronological order, oldest to newest.

Unless otherwise noted, each new release includes the software fixes added in all previous releases.

Release K.11.11 was the first production software release for the ProCurve 3500yl, 6200yl, and 5400zl Series switches. Release K.11.69 is the last release of the K.11.*xx* software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.00 code branch with no intervening releases.

The first production software release for the 8212zl switch is K.12.31.

Release K.12.57 is the last K.12.xx release prior to the roll to the K.13.xx software. Fixes added to the K.12.xx software branch after K.12.57 are therefore included in the K.13.xx software only if they are present in the itemized list of fixes for each K.13.xx build.

Release K.11.12

The following problems were resolved in release K.11.12 (never released)

- **ACL/QoS (PR_1000317233)** — Under some circumstances, the Switch may apply an ACL or QoS configuration setting incorrectly.
- **Configuration/Security (PR_1000316441)** — Operator level can save Manager privilege level changes to the configuration.
- **Crash Log (PR_1000309533)** — Incorrect crash message displayed in the log, **"**Too many HSL interrupts".
- **Crash (PR_1000317489)** — Changing the QoS/ACL portion of the running configuration may cause a switch module to crash with a message similar to:

  ```
  CL Int status=0x10000000
  ```

- **Gig-T SFP Modules (PR_1000316433)** — The switch accepts a Gig-T SFP dual personality module when it should not accept these modules.w
- **Help file enhancement (PR_1000300491)** — Added support for Help files. Switch can provide a navigation pane on the left side of the screen containing 'Contents' and 'Search' capability.
- **10 Gig Transceiver (PR_1000317965)** — Switch reports incorrect Link status when a defective fiber cable is connected to the Switch.
- **LED (PR_1000316434)** — If a mini-GBIC is installed during switch bootup, that port's link LED will not turn on.
- **MSTP Enhancement (PR_1000310463)** — Implementation of legacy path cost MIB and CLI option for MSTP.
- **RSTP (PR_1000307278)** — Replacing an 802.1D bridge device with an end node (non-STP device) on the same Switch port, can result in the RSTP Switch sending TCNs.
- **Web UI (PR_1000303371)** — In the Web User Interface, the QOS Device Priority window scroll bar does not allow sufficient scrolling to view all entries.
- **Web UI (PR_1000311917)** — When the last port on the last card is configured in a trunk or mesh, and a user browses to a specific location in the Web user interface, the HTTP Web server degrades the switch, causing the Web user interface to hang.

Release K.11.13

The following problems were resolved in release K.11.13 (never released)

- **Routing (PR_1000306239)** — In some cases, the command '**show ip route**' may display incorrect information.
- **Self-test (PR_1000315509)** — The self-test LED does not turn off after bootup of an empty chassis.
- **sFlow (PR_1000317785)** — Using Inmon Traffic Server, traffic will be reported on ports with no traffic present. Other ports may or may not have faulty counter reports.

Release K.11.14

The following problems were resolved in release K.11.14 (never released)

- **SNMP (PR_1000315054)** — SNMP security violations are entering the switch syslog when a valid SNMPv3 'get' operation is initiated.
- **Web (PR_1000302713)** — When using the Web interface and a large amount of stacking interactions occur, portions of the information from the stack commander may no longer appear.

Release K.11.15

The following problems were resolved in release K.11.15 (never released)

- **CLI (PR_1000298299)** — After a reboot, the Switch does not provide warning that the running configuration and startup configuration differ, and does not offer an option to save the running configuration.
- **CLI (PR_1000315256)** — Inconsistent error message, "`Resource unavailable`," when configuring more than the maximum number of allowed static IP routes.
- **Crash (PR_1000322009)**— The Switch may crash with a message similar to:

  ```
  Software exception in ISR at queues.c:123.
  ```

- **Menu (PR_1000318531)** — When using the Menu interface, the Switch hostname may be displayed incorrectly.

Release K.11.16

The following problems were resolved in release K.11.16 (not a general release)

- **10 GbE module (PR_1000321201)** — At a high temperature and with long cables, the Switch 3500yl X2/CX4 10-GbE module (J8694A) may not work properly.

Release K.11.17

The following problems were resolved in release K.11.17

- **Stacking (PR_1000298299)** - The Stack Commander setting is not written to the configuration file, so Web/Stacking does not work.

Release K.11.32

The following problems were resolved in release K.11.32

- **Authentication (PR_1000334731)** — PEAP/TLS EAP types with IAS Radius Server fail to authenticate.
- **CLI (PR_1000298038)** — The command "**show arp**" displays incomplete information.
- **CLI (PR_1000308346)** — The command "**show tech**" failed to execute.
- **CLI (PR_1000308601)** — The Stack Close Up device view does not display all stack members.
- **CLI (PR_1000329325)** — Unrecognizable characters printed to console on User Authentication timeout when logging in via TACAS server.
- **CLI (PR_1000329977)** — User is unable to edit any SNMPv3 target address entries.
- **Config (PR_1000326255)** — The stacking interval setting does not appear in the startup or running configuration files.
- **Crash (PR_1000228633)** — The Switch may crash with a message similar to:

  ```
  Software exception at ldbal_cost.c:1577 -- in 'eDrvPoll', task ID = 0x1760650-> ASSERT:
  failed.
  ```

- **Crash (PR_1000314305)** — The switch may crash with a message similar to:

  ```
  Software exception at ipamMApi.c:1592/1594 -- in 'eRouteCtrl'
  ```

- **Crash (PR_1000323759)** — The Switch may crash with a message similar to:

  ```
  TLB Miss: Virtual Addr=0x00000185 IP=0x8027ae04 Task='mLACPCtrl'
  Task ID=0x81597410 fp:0x00000000 sp:0x815972d0 ra:0x8027aa90 sr:0x1000fc01.
  ```

- **Crash (PR_1000324041)** — A module may crash due to ACL Parity Interrupt with a message similar to

  ```
  'ACL Int stats=0x1000000 28=0x80000b2'.
  ```

- **Crash (PR_1000325030)** — The Switch may crash with a message similar to:

  ```
  'Software exception at vls_dyn_reconfig.c:1939 -- in 'mLpmgrCtrl', task ID = 0xa139a80'.
  ```

- **Crash (PR_1000325540)** — The Switch may crash with a message similar to:

  ```
  Software exception at sw_sem.c:712 -- in 'mSnmpCtrl.
  ```

- **Crash (PR_1000327132)** — The Switch may crash with a message similar to:

  ```
  Software exception in ISR at btmDmaApi.c:304.
  ```

- **Crash (PR_1000329818)** — The Switch may crash with a message similar to:

  ```
  assert in btmDmaApi.c:289 - out of msgs, need to throttle rmon & syslog msgs.
  ```

- **Crash (PR_1000330009)** — The Switch may crash with a message similar to:

  ```
  slave assert at bttfSlaveLearn.c:1426 - extended bcast loop condition.
  ```

- **Crash (PR_1000332703)** — The Switch may crash with a message similar to:

  ```
  slave assert at ngDmaRx.c:495 - ease sample outbound received a fragment.
  ```

- **Crash (PR_1000329485)** — Broadcast loop creates additional packets causing throughput traffic to decrease.
- **Crash/ACL (PR_1000332850)** — When authenticating using Radius ACLS, configuring and un-configuring multiple ACLs may cause the Switch to crash.

- **Crash (PR_1000334992)** — The Switch may crash with a message similar to:
  `"Software exception in ISR at btmDmaApi.c:289 -> No resources available".`
- **Crash (PR_1000335430)** — The Switch may crash with a message similar to:
  `"Cam range reservation error" crash at aqSlaveRanges.c:172.`
- **Event Log (PR_1000308669)** — After a Switch reset, the event log does not display correct information.
- **Event Log (PR_1000310958)** — Unsupported modules do not produce an event log message in the Switch.
- **Fault LED (PR_1000314005)** — Upon a fan fault, the fault LED does not indicate an error.
- **Flash Memory (PR_1000320941)** — An incorrect error message is displayed when the Switch experiences a Flash memory failure.
- **Flow Control (PR_1000333879)** — Flow Control not functioning properly.
- **Help Menu (PR_1000307772)** — The Help menu text for command "router pim rp-candidate hold-time" displayed incorrect values.
- **Help Menu (PR_1000326670)** — Web User Interface Help file link URLs exceed maximum length.
- **ICMP (PR_1000315805)** — When the Switch receives a UDP packet on a closed port, Switch fails to send an ICMP response message back to the sender.
- **ICMP/Rate Limiting (PR_1000319946)** — Configuring ICMP Rate Limiting on interfaces causes the Switch to create duplicate requests, which affects the total throughput of the blade.
- **LED (PR_1000325259)** — Test LED flashing wrong color when a defective Mini-GBIC is installed.
- **LLDP (PR_1000319356)** — LLDP does not discover CDPv2 devices.
- **MAC Authentication (PR_1000329738)** — Switch may improperly flush the ARP cache when adding or removing an authorized MAC address.
- **MAC Authentication (PR_1000335314)** — While authenticating multiple ports via MAC authentication, the Switch successfully authenticates the port but fails to learn the source MAC address.
- **Meshing (PR_1000325260)** — With meshing enabled, it is possible that packet buffers may get corrupted resulting in a Switch reboot.
- **Module (PR_1000307404)** — With no cable attached, the X2 CX4 transceiver link LED remains on after a switch power up or hot swap of module.
- **Modules (PR_1000314454)** — Blades fail to reboot (retry) after failing a selftest.
- **Module (PR_1000330312)** — Booting up the Switch with an unsupported module installed may cause all existing modules to fail.
- **MSTP Enhancement (PR_1000331792)** — Implementation of Spanning-tree BPDU Filter and SNMP Traps.
- **Power Supply (PR_1000310159)** — After power supply failovers, the Switch incorrectly reports power being available on ports that are actually powered down.
- **QoS/Rate Limiting (PR_1000319946)** — QoS/Rate limiting may stop working or impact unwanted traffic streams.
- **QOS (PR_1000325028)** — Switch may crash after configuring QOS device-priority.
- **SNMPv3 (PR_1000325021)** — SNMPv3 lines may mistakenly be removed from the configuration file.
- **STP (PR_1000333992)** — In a redundant STP network with PIM running, PIM packets may get assigned a higher queue priority than STP packets, which may cause network loops.

- **Switch (PR_1000327506)** — Fixed issue where Switch incorrectly allowed jumbos frames to be configured for 10/100 ports.
- **VLAN (PR_1000334107)** — User is unable to add a port to a VLAN and the Switch responds with an invalid error message.
- **Web UI (PR_1000308213)** — Removed Web Stacking Tab within the Web User Interface for the 5400zl products.
- **Web UI (PR_1000308225)** — When using the Web User Interface, the device view of the Stack Close-up is missing.
- **Web UI (PR_1000311087)** — Serial number for 5400zl products within the Web-UI exceeds the provided rectangle.
- **Web UI (PR_1000322777)** — When using the Web User Interface in the Configuration Tab, a user is unable to modify a port name.
- **Web UI (PR_1000329279)** — When using the Web user interface Commander's Stack Close Up view, some stack members are not displayed.

Release K.11.33

The following problems were resolved in release K.11.33

- **Buffer Leak (PR_1000336963)** — The Switch may run out of packet buffers under certain conditions.
- **Crash/ACL (PR_1000337717)** — The Switch may crash with a message similar to:

  `"Software exception at alloc_free.c:422 -- in 'eDrvPoll'...-> No msg buffer", when Switch is configured for ACL logging.`
- **Module J8705A (PR_1000336281)** — The Switch 5400zl 20P 10/100/1000 + 4 mini GBIC module (J8705A) may stop forwarding packets.

Release K.11.34

The following problems were resolved in release K.11.34 (not a general release)

- **CLI (PR_1000323423)** — Entering an incorrect password three times for either the operator or manager levels causes the CLI to display erroneous characters.
- **CLI (PR_1000322029)** — The command "**show vlans**" does not display data correctly in the status field.
- **IDM (PR_1000334365)** — Using EAP/802.1x with IDM ACLs can result in memory leaks.
- **Management (PR_1000337447)** — The switch is unmanageable using Telnet or SNMP.
- **OSPF (PR_1000339542)** — When using the "**show IP route"** or "**show ip route ospf"** commands after configuring an AS External LSA (type 5) with a configured metric, the "show" commands display an incorrect metric value.
- **Web UI (PR_1000331431)** — The QoS Configuration Tab does not work correctly when using the Web User Interface.

Release K.11.35

The following problems were resolved in release K.11.35 (never released)

- **Authentication (PR_1000343377**) — When running the Windows XP 802.1x supplicant and the switch sends a re-authentication, Windows XP prompts the user to re-enter their username and password again.

- **Authentication (PR_1000344961)** — A port with multiple 802.1x users on it will allow traffic to pass for a user after that user's supplicant has been stopped.
- **DHCP (PR_1000323679)** — Client cannot obtain an IP address when two DHCP servers are connected on different local networks.
- **Enhancement (PR_1000336169)** — Added support for STP Per-Port BPDU Filtering and SNMP Traps.
- **Enhancement (PR_1000311957)** — Added an option to configure the switch to use the management VLAN IP address in the Option 82 field for all DHCP requests received from various VLANs.
- **MIB (PR_1000307831)** — The MIB value for **ipAddrTable** is not populated.
- **RIP (PR_1000331536)** — RIP does not send a route poison update in response to a failed route.
- **Show tech (PR_1000294072)** — Show Tech statistics displays incorrect port names for fixed ports.

Release K.11.36

The following problems were resolved in release K.11.36 (never released)

- **10-GbE (PR_1000346107)** — The guaranteed minimum bandwidth feature is not working on 10-GbE ports.

Release K.11.37

The following problems were resolved in release K.11.37 (not a general release)

- **Login (PR_1000347300)** — Login failures do not result in an "Invalid Password" response.

Release K.11.38

The following problems were resolved in release K.11.38 (never released)

- **10-GbE (PR_1000346107)** — The Guaranteed minimum bandwidth feature does not work on 10-GbE ports.
- **CLI (PR_1000305349)** — The command, **no ip router-id**, does not work. Once a router-ID is set, there is no way to remove it.
- **QoS (PR_1000346708)** — IP-Precedence does not set the correct priority if all TOS bits are set to 1.

Release K.11.39

The following problems were resolved in release K.11.39 (never released)

- **Crash (PR_1000344998)** — The switch may crash with a message similar to

  ```
  Software exception at sme.c:103 -- in 'mSess1', task ID = 0x8e05520
  -> ASSERT:  failed
  ```

- **Crash (PR_1000351693)** — The switch may crash with a message similar to

  ```
  Software Exception at rt_table.c.758 --  in 'eRouteCtrl', task ID = 0x8a d6b30 -> Routing
  Task: Route Destinations exceeded
  ```

Release K.11.40

The following problems were resolved in release K.11.40 (not a general release)

- **CLI (PR_1000353548)** — Use of the command **show span** incorrectly displays an error,

  ```
  "STP version was changed. To activate the change you must save the configuration to flash
  and reboot the device."
  ```

- **Crash (PR_1000352922)** — The switch may crash with a message similar to

  ```
  mstp_ptx_sm.c:118 -- in 'mMstpCtrl', task ID = 0x8899e70 -> ASSERT:  failed
  ```

- **Enhancement (PR_1000346164)** — RSTP/MSTP BPDU Protection: When this feature is enabled on a port, the switch will disable (drop the link) a port that receives a spanning tree BPDU, log a message, and optionally, send an SNMP TRAP.

Release K.11.41

The following problems were resolved in release K.11.41

- **Enhancement (PR_1000344652)** — Added support for Unidirectional Fiber Break Detection.
- **Hang (PR_1000346328)** — Switch hangs during initialization, switch may fail to boot. RMON alarms/events configuration files corrupted.
- **MDI/MDI-X (PR_1000354050)** — Forced MDI and MDIX modes were reversed on the 3500yl - forced MDI was transmitting out pins 3 and 6 instead of 1 and 2, and vice versa.
- **Port Monitoring (PR_1000354067)** — The CLI does not allow users to mirror mesh ports, resulting in "Error setting value monitor for port <n>".
- **SSH (PR_1000350999)** — The SSH login prompts user to "press any key to continue" twice before providing a prompt.
- **Web-UI (PR_1000354104)** — The Web-UI limited the size of the "Common Name" field in the SSL configuration tab to 16 characters

Release K.11.43

Version K.11.42 was never released.

The following problems were resolved in release K.11.43 (not a general release)

- **Crash (PR_1000307842)** — When deleting/removing CLI ACLs, IDM ACLs, management VLAN, or virus throttle lockouts, switch crashes with error similar to:

  ```
  ″Delete virtual meter with nonzero rule RefCount″.
  ```

- **Crash (PR_1000334982)** — When Web authentication is used with open VLANs, a software exception may occur, with the switch reporting something similar to this.

  ```
  Software exception at wma_vlan_sm.c:289 -- in 'mWebAuth',
  task ID = 0x81e408e0 -> ASSERT: failed
  ```

- **Enhancement (PR_1000358903)** — 802.1X Controlled Directions enhancement. With this change, Administrators can use “Wake-on-LAN” with computers that are connected to ports configured for 802.1X authentication.

- **VRRP (PR_1000356388)** — VRRP returns the physical MAC address instead of the virtual MAC address when replying with proxy-ARP.

Release K.11.44

The following problems were resolved in release K.11.44 (not a general release)

- **Enhancement (PR_1000361504)** — This enhancement allows STP to detect and block network topology loops on a single port.

Release K.11.46

Version K.11.45 was never released.

The following problems were resolved in release K.11.46 (not a general release)

- **CLI (PR_1000345301)** — The output from the "show config state" CLI command doesn't always report changes made to the configuration.
- **CLI (PR_1000305584)** — The output from the "show power" commands on the ProCurve 3500yl switches references slot letters when it should display port numbers.
- **Crash (PR_1000357083)** — The switch management may run out of packet buffers and crash with a message similar to:

  ```
  Software exception at ngDmaTx.c:722 -- in 'tDevPollTx', task ID = 0x4305c504 -> HW DMA DRIVER unable.
  ```

- **Hang (PR_1000359640)** — The switch may hang on initialization and become unresponsive.

Release K.11.47

The following problems were resolved in release K.11.47 (not a general release)

- **Management VLAN (PR_1000299387)** — The management VLAN does not allow connectivity from valid addresses.
- **SNMP (PR_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.

Release K.11.48

The following problems were resolved in release K.11.48 (not a general release)

- **CLI (PR_1000345301)** — The output from the "show config state" CLI command doesn't always report changes made to the configuration.
- **Crash (PR_1000334710)** — When saving changes to the IGMP configuration, the switch may crash with a message similar to this.

  ```
  TLB Miss:  Virtual Addr=0x00000000 IP=0x80591238 Task='mSess1'
  ```

- **Crash (PR_1000351243)** — The switch may crash at boot-up if more than 1000 VLANs are configured.

- **Enhancement (PR_1000351445)** — The "show tech transceiver" CLI command output now contains the HP part number and revision information for all transceivers on the switch.
- **OSPF (PR_1000363648)** — The "restrict" CLI command in OSPF redistribution does not filter the default route.

Release K.11.49

The following problems were resolved in release K.11.49 (not a general release)

- **802.1X (PR_1000358534)** — For the Controlled Directions feature of 802.1X to operate correctly, spanning tree must be enabled and authenticator ports must be set as edge ports. This fix removes a limitation that requires these steps be done in a specific order.
- **Crash (PR_1000346971)** — When stacking is disabled, the switch may crash with a message similar to:

  ```
  PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x08895e48 HW Addr=0x39200000 IP=0x007132f8
  Task='mSnmpCtrl'
  ```

- **Enhancement (PR_1000366744)** — DHCP Protection enhancement. For more information about this feature, please watch the ProCurve Web site.
- **sFlow (PR_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.

Release K.11.61

Versions K.11.50 through K.11.59 were never built.

Version K.11.60 was never released.

The following problems were resolved in release K.11.61 (not a general release)

- **802.1X (PR_1000367404)** — Increased the maximum number of 802.1X users per port to 32.
- **Crash (PR_1000366583)** — When a large config is saved using the "write memory" CLI command, the switch may crash with a message similar to:

  ```
  NMI event SW:IP=0x00897870 MSR:0x00029210 LR:0x00100c80 Task='mSess1'
  Task ID=0x8d13fe0.
  ```

Release K.11.62

The following problems were resolved in release K.11.62 (not a general release)

- **ACL (PR_1000368901)** — Outbound access control lists (ACLs) do not function after a reboot.
- **Authorization (PR_1000365285)** — IP Authorized Managers feature behaves incorrectly with regard to Telnet access.
- **CLI (PR_1000313916)** — The CLI output for the "show ip" command is misaligned; the proxy-arp column is shifted over to the left by one.
- **Crash (PR_1000356446)** — When traffic monitoring is in use, the switch may crash with a message similar to this.

  ```
  Data Bus Error: Addr=0x704a6114 Data=0x00000011 flags=0x10000751, IP=0x4012eaac
  Task='mEaseUpdt' TaskID=0x42fef338
  ```

- **Routing (PR_1000350144)** — Adding a VLAN and assigning an IP address to that VLAN through the menu interface takes routing information protocol (RIP) offline in all VLANs.
- **sFlow (PR_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.
- **VLAN (PR_1000356062)** — When configuring from the menu interface, the 3500yl series switches will not allow the following name format for a new VLAN:

  "VLANx" (where "x" is a VLAN number).

Release K.11.63

The following problems were resolved in release K.11.63

- **802.1p QoS (PR_1000368188)** — 802.1p prioritization may not work once a trunk is enabled on a module, unless the user issues the commands "qos type-of service ip-precedence" or "qos type-of service diff-services".
- **Crash (PR_1000368540)** — The switch may crash with a message similar to:

  ```
  Software exception at parser.c:8012 -- in 'mSess2',
  task ID = 0x90e10e0 -> ASSERT: failed.
  ```

- **Menu/Event Log (PR_1000319407)** — Disabling of event log numbers, via the "no log-numbers" CLI command, doesn't work properly when viewing the event log via the Menu. Using the 'next' and 'prev' buttons causes the log numbers to reappear.
- **PCM Traffic Monitoring/Performance Degradation (PR_1000370061)** — The switch is affected by PCM traffic monitoring, causing throughput degradation.
- **RADIUS (PR_1000358525)** — Attributes that were overridden by RADIUS (CoS, Rate, and ACL) remain active if an authenticated user fails to send EAP-LOGOFF.

Release K.11.64

The following problems were resolved in release K.11.64 (not a general release)

- **Crash (PR_1000372604)** — When multiple of instances of sFlow have been configured via the CLI, the switch may crash with an error similar to:

  ```
  Software exception at sflow.c:1170 -- in 'mEaseCtrl',
  task ID = 0x80e5fe0-> ASSERT:  failed.
  ```

- **Enhancement (PR_1000376406)** — Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- **Event Log (PR_1000373796)** — Selecting "Save", within the IP Configuration screen of the Menu causes unnecessary Event Log messages.
- **sFlow/Flow-Control (PR_1000375851)** — To protect performance if Flow-Control is enabled on any one or more ports, egress sFlow sampling will be disabled on all ports and a CLI/Event Log message will be generated.
- **VLAN/CLI (PR_1000368900)** — VLAN names over 12 characters in length cause the output from the command "show ip route" to be displayed incorrectly.

Release K.11.65

The following problems were resolved in release K.11.65 (not a general release)

- **Alarms/Log (PR_1000371908)** — The ambient temperature measured by the 5406zl chassis is 4 degrees C too high, causing the generation of false high temperature alarms.
- **CLI (PR_1000377318)** — The output from the CLI command, 'show dhcp-relay' is truncated.
- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the "show tech" command output.
- **Menu/Counters (PR_1000370619)** — The Menu Interface does not reflect changes to SNMP OIDs for "IP Mgmt - Tx/Rx" counters; the counter always reads "0."
- **Syslog (PR_1000379802)** — Forwarding of event log message to a configured syslog server is not disabled when a specific event log message has been disabled via the MIB.
- **VRRP (PR_1000380627)** — VRRP packets are received on a non-VRRP VLAN causing excessive event log/syslog messages.

Release K.11.66

The following problems were resolved in release K.11.66 (not a general release)

- **CLI (PR_1000379455)** — The output from some CLI "show" commands produces incorrectly formatted output on the screen.
- **CLI (PR_1000309983)** — Using the "show tech" command immediately after boot and before the modules have initialized causes the command to fail, and leaves the user in an unsupported CLI state.
- **CLI (PR_1000364628)** — The command output from "show ip rip peer" yields an improperly formatted peer IP address.
- **Meshing (PR_1000386393)** — A 5412zl switch may crash with a bus error, when 4 Port CX4 module (J8708A) in Slot L is configured for Meshing. The crash message is similar to the following.

  ```
  PPC Data Storage (Bus Error) exception vector 0x300:
  Stack Frame=0x08af5298 HW Addr=0x4b5a697c IP=0x00372ed8 Task='mLdBalCtrl' Task 0 fp:
  0x00000018
  ```

- **sFlow (PR_1000378885)** — The sFlow samplePool for trunks is sometimes unchanged between samples. This may cause inaccurate spikes in traffic monitoring applications that measure the utilization on trunk ports.
- **Web/RADIUS (PR_1000368520)** — Web Authentication doesn't authenticate clients due to a failure to send RADIUS requests to the configured server.
- **WebUI (PR_1000371598)** — Unable to Access Stack Members through Commander WebUI. Use of the WebUI "stack access" drop-down list on the stacking commander returns a "Page not found" error.

Release K.11.67

The following problems were resolved in release K.11.67 (not a general release)

- **MSTP (PR_1000385573)** — MSTP instability when root switch priority is changed. This causes other switches with better priority to assert themselves as root, thus causing a root war to occur.

Release K.11.68

Software never released.

- **CLI/LLDP (PR_1000377191)** — Output from the CLI command, "show lldp info remote-device <port>" shows a blank field for the chassis ID.
- **Crash (PR_1000390591)** — Software exception at sflow.c:3903 after re-starting sflow sampling. Switch may crash with a message similar to:

  ```
  Software exception at sflow.c:3903 -- in 'mSnmpEvt',
  task ID = 0x8248e90-> ASSERT: failed
  ```

- **DHCP (PR_1000386886)** — DHCP-relay uses an inconsistent address when the VLAN is multinetted. This fix forces the lowest IP address to be used for DHCP.
- **Enhancement (PR_1000388709)** — SFlow does not accommodate bursty traffic.
- **ROM update (PR_1000390486)** — ROM update to version K.11.03, required to support the upcoming K.12 software update.
- **Trunking (PR_1000238829)** — Trunks numbered trk10 and greater cause the output from the CLI command "show span" output to be misaligned.

Release K.11.69

The following problems were resolved in release K.11.69

- **Routing (PR_1000392086)** — The switch learns a bogus MAC address when the next hop address is unknown, causing the switch to stop forwarding traffic.

Release K.11.69 is the last release of the K.11.*xx* software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.0*x* code branch with no intervening releases.

Release K.12.01

The following problems were resolved in release K.12.01

- **ACL (PR_1000393287)** — When the same ACL is applied (in or out) to more than 2 VLANs it does not get applied to the third VLAN or higher.
- **ACL (PR_1000389442)** — Numbering restrictions are not enforced at the CLI; ACLs numbered 200 or higher are considered valid. This fix enforces ACL numbering restrictions and converts existing ACLs numbered 200 or higher into named ACLs. If an invalid name of form XXX is found, it will be converted to "invalidXXX".

  Note:

  If you have ACLs configured with numbers greater than or equal to 200, you need to reconfigure those ACLs with either a valid name or valid number prior to loading K.12.01 software, or it will be tagged as invalid. For example, if you have an ACL called 222 and it is applied to a vlan, the K.12.01 script will convert the 222 ACL to "invalid222" and apply it to the vlan.

- **CLI (PR_1000332352)** — The output of a **show int brief** command should show the negotiated flow control status rather than the flow control configuration setting.

- **Crash (PR_1000385237)** — Applying an access control list with more than 105 entries to a VLAN interface causes the switch to crash with a message similar to:

  ```
  Software exception at enDecode.c:54 -- in 'mSess1',
  task ID = 0x8e7da60 -> out of memory!
  ```

- **Crash (PR_1000392105)** — Specific actions in the port status screen of the menu interface may trigger a crash. Scrolling down to the ports on a module in slot L and pressing [enter] may cause the switch to crash with a message similar to:

  ```
  Software exception at exception.c:424 -- in 'mSess1',
  task ID = 0x8dd1ab0 -> Memory system error at 0x881a480 - memPartFree
  ```

- **Enhancement (PR_1000298920)** — A ping request issued to a VLAN which is down will now return a more specific message; instead of "request timed out", the message "The destination address is unreachable" will be displayed.

- **Enhancement (PR_1000373226)** — Support was added for the ProCurve 100-FX SFP-LC Transceiver (J9054B).

- **Enhancement (PR_1000376626)** — Enhance CLI **qos dscp-map help** and **show dscp-map** text to warn the user that inbound classification based on DSCP codepoints only occurs if **qos type-of-service diff-services** is also configured.

- **Event Log (PR_1000330310)** — Failed attempts to communicate with an unknown module type fill the event log message buffer.

- **Routing (PR_1000359162)** — When the user configures a static route that overlaps with a local subnet configured on the switch, the router will not respond to packets destined for its own IP address. The packets for its own IP address will be routed using the configured static route.

- **OSPF (PR_1000374003)** — The switch assigns itself a router-id of the neighbor router's in a virtual link.

  Note:

  Existing OSPF virtual link configurations may be lost with the update to K.12.01. Either save the K.11 configuration and reload it once the switch is running K.12, or plan to reconfigure any virtual links at the CLI after booting into the K.12.01 software.

- **SNMP (PR_1000392847)** — RMON alarms that monitor port-specific OIDs are lost if the switch is rebooted.

Release K.12.02

The following problems were resolved in release K.12.02

- **Crash (PR_1000398746)** — The switch may crash with the task "swInitTask". This could result in repeated crashes until the switch configuration is cleared.

- **Crash/Traffic Monitoring (PR_1000396662)** — When Traffic Monitoring is enabled on the switch by a network management station (such as PCM) the switch may crash with a message similar to:

  ```
  Data Bus Error: Addr=0x704a613c Data=0xffffffff flags=0x10000750, IP=0x4012fa80
  Task='tSvcWorkQ' TaskID=0x44b42ad0 cpsr=0x80000013
  ```

- **Crash (PR_1000392863)** — Switch may crash when **setmib tcpConnState** is used, with a message similar to:

  ```
  NMI event SW:IP=0x0079f4a0 MSR:0x00029210 LR:0x006dca60 Task='eTelnetd' Task
  ID=0x8a7cbb0 cr: 0x20000042 sp:0x08a7c870
  ```

- **Daylight savings (PR_1000364740)** — Due to the passage of the Energy Policy Act of 2005, Pub. L. no. 109-58, 119 Stat 594 (2005), starting in March 2007 daylight time in the United States will begin on the second Sunday in March and end on the first Sunday in November.

- **DHCP (PR_1000397753)** — A unicast DHCP request that has already been relayed by another router is sometimes dropped.
- **Hang (PR_1000397964)** — The switch appears to hang where all routing stops, the switch cannot ping anything, even addresses configured locally.
- **Proxy-ARP (PR_1000393571)** — Proxy-ARP sends responses to gratuitous ARPs.
- **Remote Mirroring/Trunking (PR_1000397196)** — Remote mirroring configured on a trunk does not restart after the switch is rebooted. Workaround: after a switch reboot, reconfigure the trunk remote as a mirroring source.
- **RIP (PR_1000393366)** — The switch does not process RIP (v2) responses containing subnets with a classful subnet mask, when the receiving RIP switch has a connected VLSM network defined that would fall within that classful range.

Release K.12.03

The following problems were resolved in release K.12.03 (not a general release)

- **CLI (PR_1000373443)** — The CLI **update** command help text and confirmation message is misleading and confusing.
- **Crash (PR_1000399448)** — Changes to traffic monitoring settings may trigger the switch to crash with a message similar to:

  ```
  Software exception at ease_ctrl.c:575 -- in 'mEaseCtrl',
  task ID = 0x8347161
  ```

- **Crash (PR_1000401664)** — Use of the CLI command **dir** with a very large path name may cause the switch to crash with a message similar to:

  ```
  PC Data Storage (Bus Error) exception vector 0x300:
  Stack Frame=0x08e54928 HW Addr=0x00b3eefc IP=0x0018a740
  Task='mSess2' Task ID=00 fp: 0x00000000 sp:
  ```

- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the **show tech** command output.
- **Enhancement (PR_1000398393)** — For the **interface <*port-list*> speed-duplex** command, added the **auto-10-100** configuration option to constrain a link to 10/100 Mbps speed and allow a more rapid linkup process when 1000 Mbps operation is not possible.
- **Enhancement (PR_1000404544)** — Provides TCP/UDP port range prioritization in the **qos** command; the **range** option assigns an 802.1p priority to (IPv4) TCP or UDP packets associated with a range of TCP/UDP ports.

Release K.12.04

Software never released.

- **ACL (PR_1000402901)** — The ACL resequencing feature may discard some ACEs in a random fashion.
- **CLI (PR_1000403104)** — Executing the **erase startup-configuration** command and rebooting does not clean up the RMON 'alarm' table.
- **Crash (PR_1000405465)** — Use of dynamically assigned ACLs may cause the switch to reboot with the following error:

  ```
  Software exception at aclBttfMUtils.c:1208 -- in 'midmCtrl',
  task ID = 0x85f6a60 -> internal error
  ```

- **Enhancement MSTP (PR_1000369492)** — Update of MSTP implementation to the latest IEEE P802.1Q-REV/D5.0 specification to stay in compliance with the protocol evolution.

Note The updated standard provides auto-edge-port operation for MSTP, and supports the automatic detection of edge ports. The port will look for BPDUs for 3 seconds; if there are none, it begins forwarding packets. For more information on selected configuration options and updated MSTP port parameters, see "Release K.12.04 Enhancements" on page 29.

- **Remote Mirroring/SNMP (PR_1000395595)** — Removing a VLAN via SNMP does not remove the related ACL relationship to that VLAN.
- **sFlow (PR_1000408145)** — sFlow samples for routed packets do not occur bidirectionally; inbound packets are dropped and only outbound packets are sampled.
- **Traceroute (PR_1000379199)** — The reported **traceroute** time is inaccurate; it is one decimal place off.

Release K.12.05

The following problems were resolved in release K.12.05.

- **BootROM (PR_1000402707)** — BootROM does not update to latest version when updating code to primary flash.
- **CLI (PR_1000309998)** — Management module is incorrectly displayed as J8627A rather than the correct J8726A product number in response to the **show modules** command.
- **Enhancement (PR_1000408960)** — RADIUS-Assigned GVRP VLANs enhancement. For more information, see "Release K.12.05 Enhancements" on page 29.
- **Menu (PR_1000392862)** — The menu will allow invalid values (greater than 720 sec) to be entered for the SNTP poll interval.

Release K.12.06

Software never released.

- **Enhancement (PR_1000308332)** — Passwords (hashed) are saved to the configuration file. For more information, see "Release K.12.06 Enhancements" on page 29.

Release K.12.07

The following problems were resolved in release K.12.07.

- **Config (PR_1000405639)** — Various characters in configuration file names (including dash, ampersand, plus, and spaces within quotes) result in truncated names after reboot. This is not just a display issue; the command **erase config <*filename*>** does not remove a file containing the problem characters.
- **Config (PR_1000410790)** — Errors are returned when applying the **interface <*port-list*> speed-duplex auto-10-100** command to interfaces 45 through 48 on a 3500yl-48G-PWR switch.

- **Crash (PR_1000410758)** — When the **interface <*port-list*> speed-duplex auto-10-100** command is issued on a range of ports, the switch may crash with a message similar to:

  ```
  NMI event HW:IP=0x0083f224 MSR:0x00029210 LR:0x0033c3c4 Task='tDevPollRx' Task
  ID=0x9137e50 cr: 0x20000022 sp:0x09137d78 xer:0x20000000
  ```

- **RIP (PR_1000377789)** — RIP restrict filters are not working upon reboot.
- **RMON (PR_1000410885)** — RMON alarms/thresholds set via SNMP are cleared after reboot.

Release K.12.08

Software never released.

- **Enhancement (PR_1000413764)** — Increase the size of the sysLocation and sysContact entries from 48 to 255 characters. For more information, see "Release K.12.08 Enhancements" on page 29.

Release K.12.09

The following problem was resolved in release K.12.09 (Not a general release).

- **Crash (PR_1000385844)** — With sFlow sampling enabled, the switch may crash with a message similar to:

  ```
  Software exception at ngDmaTx.c:729 -- in 'tDevPollTx',
  task ID = 0x4305bba8 -> HW DMA DRIVER unable to transmit anymore
  ```

Release K.12.10

The following problems were resolved in release K.12.10.

- **ARP (PR_1000414347)** — ARP table address learning is slow; once the switch has its ARP table cleared, the clients will be unable to communicate for approximately 30 seconds.
- **Config (PR_1000416508)** — Cannot create alternate startup-config file. Although **show config files** shows an available slot, the switch does not allow copying from an existing config file to create a new config file in the vacant slot.
- **Crash (PR_1000421322)** — Following execution of config-related CLI commands (such as **show running-config** or **show tech**) or when PCM attempts to retrieve the configuration file using TFTP from a switch having a large configuration file, the switch may crash with a message similar to:

  ```
  Software exception at exception.c:373 -- in 'tTftpDmn',
  task ID = 0x11cfaa8 -> Memory system error at 0x1175550 - memPartFree
  ```

  The following related crash message may also be addressed with this fix:

  ```
  PPC Bus Error exception vector 0x300: Stack-frame=0x016778b0
  HW Addr=0x667c4c88 IP=0x004dbc88 Task='eChassMgr'
  Task ID=0x1677dd8 fp: 0x667c4c88 sp:0x01677970 lrecpgyp
  ```

- **Enhancement (PR_1000419653)** — The **show vlan** command was enhanced to display each port in the VLAN separately, display the friendly port name (if configured), and display the VLAN mode (tagged/untagged/forbidden) for each port. For more information, see "Release K.12.10 Enhancements" on page 29.
- **SNMP (PR_1000374893)** — When retrieving the switch serial number via SNMP, the management module serial number is returned instead of the chassis serial number.

- **SNMP (PR_1000422129)** — HP Fault Finder doesn't send the interface index with the SNMP trap, even though it is listed in the system log.

Release K.12.11

Software never released.

Release K.12.12

The following problems were resolved in release K.12.12 (Not a general release).

- **Crash (PR_1000420709)** — Entering a backslash at the CLI may cause the switch to crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300:
Stack Frame=0x08e66508 HW Addr=0x00b4f2ac IP=0x0018a864 Task='mSess1' Task
ID=0x8e67170  fp: 0x3be00000 sp:
```

- **Link LED (PR_1000425143)** — The Small Form-factor Pluggable (SFP) link LED does not work when SFP is hot-swapped into the switch.

Release K.12.13

Software never released.

Release K.12.14

The following problems were resolved in release K.12.14.

- **Authentication (PR_1000422933)** — Issue with local password authentication.
- **CLI/Clear button (PR_1000424194)** — The command **no password manager** deletes the password, but fails to delete the username. Similarly, pressing the clear button deletes the password but not the username.
- **SNMP (PR_1000423362)** — Setting username via SNMP (**hpSwitchAuthMIB**) deletes the password.
- **Hotswap (PR_1000422714)** — Hotswapping a module may result in a false module self-test failure. After hotswapping the module, the following messages may appear in the event log:

```
I 05/27/06 12:06:54 00076 ports: port B23 is now on-line
W 05/27/06 12:07:00 00564 ports: port B23 PD Invalid Signature indication
I 05/27/06 12:32:47 00068 chassis: Slot B Inserted
I 05/27/06 12:32:48 00068 chassis: Slot B Inserted
I 05/27/06 12:32:49 00068 chassis: Slot B Inserted
I 05/27/06 12:32:50 00067 chassis: Slot B Removed
I 05/27/06 12:32:50 00077 ports: port B23 is now off-line
W 05/27/06 12:33:11 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:33:34 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:33:57 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:34:19 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:34:42 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
I 05/27/06 12:34:44 00179 mgr: SME CONSOLE Session - MANAGER Mode
W 05/27/06 12:35:05 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:35:05 00274 chassis: Slot B self test failure or unsupported
```

  Multiple insertion messages may be included. The errors appear in the log as either a tombstone, HSL failure, or a loss of communications.

Release K.12.15

The following problems were resolved in release K.12.15.

- **Enhancement (PR_1000427592)** — This enhancement adds the client's IP address to the RADIUS accounting packets sent to the RADIUS server by the switch.
- **Crash (PR_1000407238)** — Execution of the "show config" command when the startup configuration is different than the running configuration may cause the switch to crash with a message similar to:

  ```
  Software exception at cli_mirror.c:6201 -- in 'mSess1', task ID = 0x8e53690 -> ASSERT:
  failed
  ```

- **SNMP (PR_1000406398)** — The URL embedded SNMP traps are not sent as SSL (https) when SSL is enabled, but are sent as plain-text (http) instead. This may result in the trap receiver (such as PCM) being unable to display the URL if SSL is enabled.
- **Enhancement (PR_1000428642)** — The SNMP v2c describes two different notification-type PDUs: traps and informs. Prior to this software release, only the trap's sub-type was supported. This enhancement adds support for informs.
- **Crash (PR_1000427674)** — False positive memory testing may result in an ACL interrupt crash with an event log message similar to:

  ```
  chassis: Slot L ACL Int status=0x2000000 25=0x80000005: Task=tDevPollRx Task
  ID=0x4305d314 IP=0x40087044
  ```

- **Rate-Limiting (PR_1000420720)** — Rate limiting is broken beyond 9.5 Mbps. For any rate limit set to more than 9.5 Mbps, the actual rate drops to 1 Mbps.

Release K.12.16

The following problems were resolved in release K.12.16.

- **Crash (PR_1000415621)** — Removing a VLAN that has OSPF configured may cause the switch to crash with a message similar to:

  ```
  NMI event HW:IP=0x0084a0a4 MSR:0x00029210 LR:0x00513ee4 Task='eRouteCtrl' Task
  ID=0x89658b0'
  ```

- **Crash (PR_1000428582)** — Typing non-alphanumeric characters at the CLI prompt may cause the switch to crash with a message similar to:

  ```
  PPC Data Storage (Bus Error) exception vector 0x300:Stack Frame=0x08e36878 HW
  Addr=0x00b4f2ec IP=0x0018a974 Task='mSess1' Task ID=0x0fp: 0x18020800 sp:
  ```

Release K.12.17

The following problems were resolved in release K.12.17.

- **STP (PR_1000420442)** — The switch erroneously allows configuration of spanning tree parameters on an interface that is a member of a trunk (link aggregation group), which creates an invalid configuration.
- **CLI (PR_1000429474)** — The "all" parameter is missing from the "password" command.
- **Radius (PR_1000432556)** — When DHCP snooping is enabled on the client VLAN, and the client is on a VLAN other than the default VLAN, the Framed-IP-Address attribute is not added to the RADIUS accounting packet as it should be.

- **Crash (PR_1000416453)** — Execution of the "show tech" command in an SSH session may cause the switch to crash with a message similar to:

```
Software exception - Assert in pmgr_util.c:1155 -- in 'mSess2', task ID = 0x85adf60
```

Release K.12.18

The following problems were resolved in release K.12.18.

- **CLI (PR_1000419379)** — The “interface” command does not exist in the VLAN context, resulting in an inability to shift to the interface configuration context directly from the VLAN context.
- **Hang (PR_1000434809)** — The switch may hang, causing all the port LEDs to remain lit, and stop transmitting traffic.
- **Enhancement (PR_1000428213)** — This software enhancement adds the ability to configure a secondary authentication method to be used when the RADIUS server is unavailable for the primary port access method.
- **Crash (PR_1000436274)** — Typing a question mark ("?") at the "multi-line" input prompt (">") may cause the switch to crash. The crash occurs when the switch is trying to print the error message that states:

```
Expansion help not available on multi-line input.
```

- **CLI (PR_1000433948)** — When command authorization is in use, the "show tech" command fails at the “show tech buffer” component, even when the permission list indicates that it should be allowed.
- **Enhancement (PR_1000415155)** — The ARP age timer was enhanced from the previous limit of 240 minutes to allow for configuration of values up to 1440 minutes (24 hours) or "infinite" (99,999,999 seconds or 3.2 years).
- **Enhancement (PR_1000438015)** — The banner message of the day (MOTD) size has been increased to support up to 3070 characters.

Release K.12.19

The following problems were resolved in release K.12.19.

- **ACL (PR_1000432563)** — ACLs with the "permit" parameter on L4 ports and using operators ‘gt’/‘lt’/‘range’ do not function as expected. The ACL does not drop traffic with non-permitted L4 ports. Instead, all traffic with L4 ports is forwarded.
- **CLI (PR_1000438486**) — When using the "port-access mac-based" CLI command, the client MAC address is sent in lower case and as the username to the RADIUS server. This fix adds an option so that the MAC address is in uppercase when sent to the RADIUS server. This fix adds additional parameters to the CLI command to support this: "aaa port-access mac-based addr-format."
- **10-GbE Log (PR_1000424384)** — The switch is not checking for the presence of the J8694A ProCurve yl 10G X2-CX4 module early enough in the boot process, triggering a log message when the check is executed.

Release K.12.20

The following problems were resolved in release K.12.20 (Never released.)

Release K.12.21

The following problems were resolved in release K.12.21 (never released).

- **ARP Protection (PR_1000438129)** — ARP and ARP protection data may not display correctly following a CLI or SNMP status query.
- **Enhancement (PR_1000440049)** — Classifier-Based Rate Limiting capability was added. Classifier-Based Rate Limiting (also known as Rate Limit Port ACLs or RL-PACLs) allows you to create an ACL and apply it on a per-port basis to rate-limit network traffic.
- **CLI (PR_1000342461)** — If a trunk is configured, output from the CLI command “show lldp info remote <port number>" reports incorrect information for the remote management address. This may result in a failure to discover or map devices connected to these trunks by management applications that use LLDP discovery (e.g. ProCurve Manager).
- **Enhancement (PR_1000374051)** — The 5400zl switches are not detecting packets from an Avaya G700 PBX or Cajun switch due to irregular Ethernet packets sent by those devices. This is a workaround that will alter the 5400zl software to allow 100Mb operation on the upcoming "C" revision of the 1000 Base-T Mini-GBICs (J8177C) that fit in the J8705A module. The port containing the 1000 Base-T Mini-GBIC can be configured with new speed options of "auto-100," "100-full," and "100-half."
- **Crash (PR_1000434888)** — A switch module may crash with a message similar to:

  ```
  ACL Int status=0x10000000 28=0x80002f3a: Task=tDevPollTx Task ID=0x4305c504
  IP=0x400693e8
  ```

- **Enhancement (PR_1000443349)** — This enhancement is to allow the concurrent use of SFTP with TACACS+ authentication for SSH connections.
- **VRRP/Meshing (PR_1000435853)** — A MESHed link in the path between a VRRP Owner and VRRP Backup may lead to a situation where both VRRP routers remain in Master state for a VRID after that VRID fails over to the Backup and then the Owner comes back online.
- **Routing (PR_1000432449)** — If the switch is configured with both port security and routing, a physical port transition on the host may cause the switch to stop transmitting routed traffic to that host. Clearing the ARP cache resolves this problem until another port transition occurs.
- **RADIUS (PR_1000442879)** — If RADIUS (or TACACS+) keys are configured, and then the switch is updated to a software revision with the ability to save the security credentials in the configuration file (K.12.06 or later), the RADIUS keys are no longer shown in output from the "show run” or “show config" commands until the "include-credentials" command is issued.

Release K.12.22

The following problems were resolved in release K.12.22.

- **Enhancement (PR_1000443026)** — Support for the new revision "C" Mini-GBICs was added to the CLI and the "show tech" command.
- **Enhancement (PR_1000444415)** — OSPF Passive Interface support was added.
- **Crash (PR_1000442695)** — Pasting a VRRP configuration into the running configuration via a Telnet session may cause the switch to crash with a message similar to:

  ```
  Software exception at vrrp_statemach.c:205 -- in 'mVrrpCtrl', task ID = 0x8b154a0->
  internal error
  ```

Release K.12.23

The following problems were resolved in release K.12.23.

- **Crash (PR_1000415534)** — Execution of the "lockout-mac" CLI command, may cause the switch to crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x0ab9a738 HW
Addr=0x00b3f104 IP=0x00801d2c Task='eDrvPoll' Task ID=0xab9ad20 fp: 0x0f3808c0 sp
```

- **AAA/CLI (PR_1000445886)** — This changes the syntax of '**aaa authentication** <port-access | mac-based | web-based>' commands which were previously added in PR_1000438486.
- **CLI (PR_1000403478)** — Power over Ethernet (802.3af) CLI commands were removed from platforms that do not support PoE (such as the ProCurve 6200yl switch).
- **Broadcast-limit (PR_1000429594)** — The broadcast limit feature affects multicast traffic. This fix modifies the feature so that it only affects broadcast traffic.
- **MSTP (PR_1000439775)** — The switch generates a topology change when a port goes off-line. With MSTP enabled and all ports left at default (auto-edge-port), when a port transitions to offline, a TC will be generated, and the topology change counter increases.
- **Multicast (PR_1000436118)** — Multicast forwarding with IGMP is slow and causes an unacceptable delay in servicing.
- **Enhancement (PR_1000449129)** — This enhancement allows MAC or Web-based authentication to use PEAP/MS-CHAPv2 protocols in addition to the default setting of CHAP.
- **Crash (PR_1000444112)** — Downloading a configuration file to the switch may cause a crash with a message similar to:

```
Software exception at cli_config_action.c:5479 -- in 'mftTask'
```

- **SNMP (PR_1000448463)** —The SNMP Engine ID Discovery process described in RFC 3414 is not working properly.

Release K.12.24

The following problems were resolved in release K.12.24.

- **Hang (PR_1000448429)** — A bank of ports may fail the self test, crash or stop functioning after several weeks of use. This failure may result in event log messages similar to those listed below.

```
W 06/10/07 08:07:22 00374 chassis: Ports 25-48: Lost Communications detected - Heart Beat Lost
I 06/10/07 08:07:22 00077 ports: port 31 is now off-line
I 06/10/07 08:07:22 00077 ports: port 40 is now off-line
I 06/10/07 08:07:29 00375 chassis: Ports 25-48 Downloading
I 06/10/07 08:07:30 00376 chassis: Ports 25-48 Download Complete
W 06/10/07 08:08:32 00374 chassis: Ports 25-48 Failed to boot-timeout    (AGENT_FAILED)
```

Release K.12.25

The following problems were resolved in release K.12.25.

- **Config (PR_ 1000451779)** — Software update, TFTP restoration of the configuration or reloading the switch on software version K.12.22 may delete a Mini-GBIC VLAN port assignment.

Release K.12.26 through K.12.29

Software never built.

Release K.12.30

Software never released.

Release K.12.31

The following problems were resolved in release K.12.31.

- **Enhancement** — Support for the following ProCurve product was added.

  J9091A / J8715A (bundle) for the ProCurve switch 8212zl

Release K.12.32

Never released. The following problems were resolved in build K.12.32.

- **Enhancement** — Merged all of the K.12.24 and earlier software fixes and enhancements with the ProCurve switch 8212zl support.

Release K.12.33 through K.12.40

Software never built.

Release K.12.41 through K.12.42

Software never released.

Release K.12.43

The following problems were resolved in release K.12.43.

- **Enhancement** — Support for the following ProCurve products was added.

  J9051A ProCurve Wireless Edge Services zl Module

  J9052A ProCurve Redundant Wireless Edge Services zl Module

For more information, see "Support for the Wireless Edge Services zl Module" on page 15.

Release K.12.44

Not a general release.

- **Enhancement (PR_1000457691)** — This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. For more information, see "Release K.12.44 Enhancements" on page 31.

- **Enhancement (PR_1000457868)** — Local Proxy ARP enhancement. For more information, see "Release K.12.44 Enhancements" on page 31.
- **Enhancement (PR_1000456271)** — PC attached to telephone. For more information, see "Release K.12.44 Enhancements" on page 31.

Release K.12.45

The following problems were resolved in build K.12.45. (Never Released.)

- **STP (PR_1000449365)** — ARP & MAC tables get out of sync after a spanning tree (MSTP or RSTP) re-convergence. An ARP entry fails to be associated to the port even though the MAC entry exists. This may result in an unexpected ping failure.
- **PIM (PR_1000450431)** — IP Multicast Routing PIM-DM Stops Forwarding Flows, and the event log reports:

  ```
  PIM: Failed alloc[ation] of HW Flow for flow <multicast address>
  ```

- **SSH (PR_1000453226)** — Configuration of SSH login to the manager mode (**aaa authentication ssh enable public-key** <enter>) triggers an error "Not legal combination of authentication methods", but it should be a valid command syntax.
- **Authentication (PR_1000454714)** — Concurrent 802.1X and MAC-authentication does not give the 802.1X value precedence. This fix gives 802.1X VLAN assignment precedence over MAC auth RADIUS VLAN assignment.
- **SNMP (PR_1000389902)** — The switch is not sending an "embedded URL" within the SNMP trap for an FFI event to the PCM server monitoring traps. The embedded URL, if sent, would allow someone looking at the log event on the PCM server to simply click on the URL and be immediately connected to the switch.
- **CLI (PR_1000418891)** — The Connection Rate Filter *ignore* list does not display properly in the output for the show run command; the IP address and mask are incorrectly printed on the next line.
- **SNMP (PR_1000444744)** — An *snmp set* of hpicfDot1xPaePortauth or an *snmp set* hpicfDot1xPaePortSupp of an invalid value may cause the switch to crash with a message similar to the following:

  ```
  ASSERT at aaa8021x_dyn_reconfig.c.
  ```

- **SSH (PR_1000461002) —** Issue with authentication when SSH is configured.

Release K.12.46

The following problems were resolved in build K.12.46. (Never Released.)

- **Mirroring (PR_1000458287) —** Remote mirroring does not work in slots K or L of the 5412zl or 8212zl chassis.
- **Crash (PR_1000456340) —** Switch may crash with a message similar to:

  ```
  No message buffers: alloc_free.c:435.
  ```

  The trigger for this crash is unknown, though it is suspected to be related to sFlow.

- **Module Failure (PR_1000464335) —** Switches running K.12.31 - K.12.43 may experience a problem with modules failing to boot. The system log may report a message similar to the following:

  ```
  W 11/08/05 02:43:14 00374 chassis: Slot D Failed to boot-timeout-(AGENT_FAILED)
  I 11/08/05 02:43:19 00375 chassis: Slot D Downloading
  I 11/08/05 02:43:21 00376 chassis: Slot D Download Complete
  W 11/08/05 02:44:21 00274 chassis: Slot D self test failure or unsupported module
  ```

- **Telnet hang (PR_1000457765) —** If **Ctrl+S** is typed and then the Telnet window is closed, the Telnet session may become unresponsive, and fail to reset by the **kill** command issued at the console prompt. This may require the switch to be reloaded to become active again.

Release K.12.47

The following problems were resolved in release K.12.47.

- **Enhancement Removed (PR_1000468258) —** The PC attached to IP telephone enhancement was removed. For more information, see "Release K.12.47 Enhancements" on page 31.

Release K.12.48

The following problems were resolved in release K.12.48.

- **Enhancement Removed (PR_1000470136) —** Removal of the enhancement that allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. The initial implementation of this enhancement did not allow smooth migration of pre-existing MSTP configurations. For more information, see "Release K.12.48 Enhancements" on page 31.
- **CLI (PR_1000417447) —** Some of the instrumentation monitoring parameters (e.g. arp reply monitoring) are not functioning.

Release K.12.49

The following problems were resolved in build K.12.49. (Never Released.)

- **Enhancement (PR_10004570598) —** An improved version of the MSTP-VLAN mapping enhancement referenced in PR_1000457691 was added. This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. For more information, see "Release K.12.44 Enhancements" on page 31.
- **MSTP (1000457691) —** MSTP instances are removed from the configuration after an update and reload into software version K.12.47.
- **Enhancement (PR_1000471015) —** Reintroduction of the feature referenced in PR_1000456271, that will allow a PC to connect with its RADIUS-assigned VLAN after an attached IP phone has authenticated on the authenticating port. For more information, see "Release K.12.44 Enhancements" on page 31.

Release K.12.50

The following problems were resolved in build K.12.50. (Never Released.)

- **CLI (PR_1000464787) —** Minor modifications to internal switch functions.

Release K.12.51

The following problems were resolved in release K.12.51.

- **Trunking (PR_1000461440) —** When dynamic ARP protection and DHCP snooping are configured, a trunk's *trust* status cannot be configured from the appropriate interface configuration context.

- **Routing (PR_1000424308) —** A static route that points to a deleted VLAN may cause other routing table errors.
- **CLI (PR_1000473468) —** Removing a VLAN range from an MSTP instance (e.g., no spanning-tree instance 2 vlan 10-20) fails to delete the VLANs. Listing individually the VLANs desired for deletion will correctly remove the VLANs.

Release K.12.52

The following problems were resolved in release K.12.52 (never released).

- **Enhancement (PR_1000458484) —** This enhancement allows the user to set a maximum frame size for jumbo frames at the global level. For more information, see "Release K.12.52 Enhancements" on page 32.
- **Enhancement (PR_1000461576) —** This enhancement introduces PVST Protection and Filtering. For more information, see "Release K.12.52 Enhancements" on page 32.
- **Enhancement (PR_1000462841) —** This enhancement changes the re-authentication process to allow an authenticated client to remain authenticated during re-authentication. For more information, see "Release K.12.52 Enhancements" on page 32.
- **Enhancement (PR_1000462104) —** This enhancement allows the configuration of modules not currently inserted in the switch. For more information, see "Release K.12.52 Enhancements" on page 32.
- **Enhancement (PR_1000462847) —** This enhancement allows the configuration of transceivers not currently inserted in the switch. For more information, see "Release K.12.52 Enhancements" on page 32.

Release K.12.53

The following problems were resolved in release K.12.53.

- **Crash (PR_1000472846) —** Rebooting the switch with an active Telnet session and while remote mirroring is in use may cause the switch to crash with a message similar to the following. There may also be other, unknown triggers that cause this crash.

  ```
  0x4001bf18 in fatal_exception (file=0x400a8b8c "ngDmaRx.c", line=1413, errorcode=256,
  str=0x400a8b7c "ASSERT: failed."
  ```

- **xSTP (PR_1000715227) —** When there is no module and transceiver inserted in the target slot, attempts to set up a unique path cost on the transceiver port results in an `"invalid input"` error.

Release K.12.54

The following problems were resolved in release K.12.54.

- **Connection Rate Filter (PR_1000440871) —** Some types of traffic could result in connection rate filtering (CRF) that blocks the switch management IP address.
- **Connection Rate Filter (PR_1000716601) —** Connection Rate Filtering does not remove throttled entries when filtering is disabled. The throttled host remains permanently blocked.
- **TFTP (PR_1000427390) —** When the configuration of a 6200yl switch is copied to a TFTP server, the config shows a line with the following description: `module 1 type JFIXME`. If that line is removed from the config and then the config is transferred back to the switch, the transfer will fail with the switch reporting, "`corrupted config.`" This fix results in the fixed switch ports being described as: `module 1 type J8992A`.

- **Crash (PR_1000716461) —** Loading a configuration file that uses up all the ACL resources may cause the switch to crash with a message similar to:

  ```
  NMI event SW: IP=0x007c755c MSR: 0x00029210 LR: 0x007c7544 Task='mftTask' Task
  ID=0x8a60920cr: 0x24024442 sp: 0x08a5f850 xer: 0x20000000
  ```

- **Link Speed (PR_1000432419) —** Ports 1-24 on the ProCurve 3500yl-24G-PWR and ports 25-48 on the ProCurve 3500yl-48G-PWR switches may link at 10/100 speeds rather than the gigabit speed they support.
- **TFTP (PR_1000419582) —** The switch CLI counter displays the wrong size of the file being transferred when uploading from switch flash to TFTP server. The file that is actually transferred is the correct size. This CLI display is in error.
- **PIM (PR_1000306675) —** The switch CLI does not allow the commands to remove PIM and IP multicast routing after the removal of a premium license from ProCurve 5400zl or 3500yl Series switches.
- **CLI (PR_1000447529) —** The CLI output of the command **show rate-limit all** is corrupted.
- **Manufacturing (PR_1000740632) —** Upon reload, the manufacturing information is zeroed out.

Release K.12.55

The following problems were resolved in release K.12.55 (never released).

- **DARPP (PR_1000736402) —** The last port on the switch will not be initialized with Dynamic ARP Protection (DARPP) characteristics if the last two ports are DARPP configured. For example, if the switch has 24 ports and ports 23 and 24 have DARPP characteristics, the DARPP characteristics for port 24 will not be initialized. The last port will be initialized in all other cases.
- **CLI (PR_1000340826) —** The CLI output from a **show interface** command truncates counters that have large values.
- **CLI (PR_1000742974) —** The CLI had some initial limitations within the interface context for configuration of uninserted modules and transceivers. This fix addresses the interface context for spanning-tree, aaa port-access, DHCP snooping, loop protection, and a number of other features.

Release K.12.56

The following problems were resolved in release K.12.56.

- **Enhancement (PR_1000464170) —** This feature provides support for adding the LLDP VLAN Name TLV to LLDP advertisements generated by ProCurve switches. For more information, see "Release K.12.56 Enhancements" on page 32.

Release K.12.57

The following problems were resolved in release K.12.57.

- **Enhancement (PR_1000713394) —** Adjustable IGMP Querier interval.
- **Daylight Savings Time (PR_1000467724) —** This change corrects the schedule for Western Europe Time Zone: DST to start the last Sunday in March and DST to end the last Sunday in October.
- **SSH/SCP (PR_1000742969) —** The following issues with using SSH/SCP were fixed.

  1) In **show ip ssh**, sessions 3 & 4 may display "`console`" instead of "`inactive`," when those sessions are not in use.

2) The switch does not send an appropriate exit-status message to the client. This corrects the symptom that occurs in some applications, which reports a message similar to:

```
Fatal error: Server unexpectedly closed connection.
```

3) The SSH client application does not get a command prompt (or equivalent) back from the switch until the OS is verified and burned to flash.

4) The **show flash** command incorrectly shows an OS image present in flash before the OS has completely copied to flash.

- **Routing (PR_1000744325) —** When a PC is using the switch as its default gateway, and that switch is set with a default route to another device on the same VLAN, duplication of packets may occur. Symptoms may include seeing TCP packets out of order due to retransmission.
- **ACL (PR_1000751460) —** Manipulating ACEs on a switch with the ACL applied may result in a switch hang or crash with a message similar to the following.

  ```
  SubSystem 0 went down: 11/05/07 10:16:07 Software exception at ipAccessHandle.c:161 --
  in 'mSess2', task ID = 0x876ffa0 -> internal error
  ```

- **PIM (PR_1000745983) —** PIM-Sparse Mode causes packet drops in protocols that use a destination IP multicast address such as VRRP/OSPF hello packets, and RIPv2 advertisements.
- **802.1X (PR_1000741874) —** Entering invalid 802.1X credentials (triggering failed authentication) and then trying again with valid credentials may cause the switch may crash with a message similar to the following. Symptoms and triggers for this problem may vary.

  ```
  Software exception at aaa8021x_util.c:2290 -- in 'm8021xCtrl', task ID = 0x85db0 ->
  ASSERT: failed.
  ```

- **Manufacturing (PR_1000752302) —** The ESP module does not initialize in the zl switches during the manufacturing process.
- **Connection Rate Filter (PR_1000751758) —** The “low sensitivity” connection rate filter setting was too sensitive. This fix improved the filter accuracy for "low sensitivity" levels.
- **Config (PR_1000749046) —** The running and startup configurations that are copied via TFTP do not match the output from the **show run** or **show config** output for the ProCurve 3500yl and 6200yl switches.
- **Hang (PR_1000752561) —** Multiple SNMP *get* requests over a 10-GbE link leave the switch in a problematic state. In this state one or more of the following may occur.

  1) Some CLI commands may not produce the expected output, or the output will be truncated.

  2) The **reload** command may not properly respond to some parameters.

  3) New Telnet sessions may not be allowed to form.

  4) DHCP requests may be lost by the switch.

  5) The system may need to be reloaded before the issues clear.

Release K.13.02

The following problems were resolved in release K.13.02.

- **Enhancement (PR_1000458124) —** VRRP Preemptive Delay Timer. For more information, see “Release K.13.02 Enhancements” on page 34.
- **CLI (PR_1000307590) —** Tab-help error in the spanning-tree instance <*instance number*> vlan <*vlan number*> command context.
- **CLI (PR_1000330684) —** Help text in the spanning-tree <port_id> context was updated.

- **CLI (PR_1000742426) —** The CLI command **copy usb pub-key-file** doesn't provide all the appropriate options.
- **Event Log (PR_1000751191) —** There is a misspelled event log message: `chassis: Insufficient power supplies`.
- **Event Log (PR_1000757272) —** There may be corruption in PIM log messages.
- **DHCP Snooping (PR_1000757935) —** DHCP Snooping may miss some packets in certain situations.
- **Mirroring (PR_1000758793) —** When a mirror ACL is applied with multiple destinations, only one of those destinations work properly. Beginning with K.13.02 software, there is only one ACL mirror destination supported.
- **Mirroring (PR_1000758803) —** Applying a second mirror ACL using the same access group number adds a conflicting mirror session rather than replacing the existing entry.
- **Mirroring (PR_1000758810) —** When an ACL used as a mirror ACL is modified, the mirror does not get updated.
- **Mirroring (PR_1000758814) —** Applying a mirror ACL may overwrite a standard mirror session (of the same number) rather than triggering an error stating that the mirror session is already in use.
- **Counters (PR_1000758834) —** SFLOW counter-polling samples may be infrequent or they may stop until the switch is rebooted.
- **IGMP (PR_1000739226) —** Some hosts or downstream devices may experience a disruption in multicast data due to the loss of IGMPv3 reports.
- **VRRP (PR_1000401050) —** Turning on IP multicast routing without enabling PIM may cause VRRP starvation.
- **SCP (PR_1000760416) —** Software transferred through SCP upload becomes corrupted; the image is successfully copied via SCP, but when the switch processes the image in copying to flash, the write never completes.
- **CLI (PR_1000455370) —** Commands that display portmaps may yield corrupted output. For example, a single port may be displayed as a port range.
- **RIP (PR_1000751858) —** Some static routes may not be correctly distributed by RIPv1 or RIPv2.
- **PIM (PR_1000714322) —** A new multicast stream may not get forwarded by the switch.
- **Crash (PR_1000759046) —** Using the "\" character with or without other character combinations may cause the switch to crash with a message similar to the following. There may also be different crash messages resulting from the same problem.

  ```
  Software exception at parser.c:2653 — in 'mSess1', task ID = 0x898e6a0-> ASSERT:  failed
  ```

- **PIM (PR_1000749627) —** A switch with PIM-SM may send a prune to the RP when none is required.
- **Web Management (PR_1000472572) —** The Web Management Interface does not properly allow configuration of port monitoring/mirroring.

Addendum to Release K.13.02:

- **ACL (PR_1000714376/1000760152) —** Attempts to apply an access group to a range of ports will fail after the initial configuration unless a write mem and reload are done in between configuration statements.

Release K.13.03

The following problems were resolved in release K.13.03.

- **Enhancement (PR_1000400991) —** The 802.1X Controlled Directions feature now functions independently of the STP configuration.

- **IPv6 (PR_1000768670) —** When virus throttling is configured on a port that belongs to an IPv6 enabled VLAN, some IPv6 all nodes (ff02::1) multicast traffic may be dropped.
- **Mirroring (PR_1000768655) —** After a mirror ACL has been modified, some ACL commands that follow may result in an unresponsive CLI session.
- **IDM ACL (PR_1000768727) —** An IDM ACL that uses the syntax, *destination ip "any"* will result in a parsing error, the ACL will not be applied, and the client authentication will fail. Workaround: Instead of the term "any," use “0.0.0.0/0.”
- **VRRP PDT (PR_1000756475) —** If the VRRP preemptive delay timer (PDT) is configured, the virtual router mode (Owner or Backup) cannot be changed unless the PDT configuration is removed.
- **Crash (PR_1000763409) —** When entering and deleting ACLs, the switch may crash with a message similar to:

  ```
  PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x087a1ba8 HW
  Addr=0x1f89d420 IP=0x005e62e0 Task=’mSess2’ Task ID=0x87a3cd0.fp: 0x00000005
  sp:0x087a1c68 lr:0x005e6340.
  ```

- **DHCP Relay (PR_1000751623) —** If the IP address on a VLAN interface is changed, any previously configured IP Helper address stops working.

Release K.13.04

The following problems were resolved in release K.13.04 (never released).

- **Self-test/Module (PR_0000000510) —** Inserting a module into a Switch 8212zl may result in the module failing to initialize with one of the following error messages:

  ```
  Self test failure or unsupported module, or
  chassis: Insufficient power supplies to power Slot <x>
  ```

- **Port/Config (PR_1000772652) —** A switch running software version K.12.52 or later only accepts the speed-duplex settings ‘auto’ or ‘1000-full’ for the dual-personality ports when the configuration file is transferred to the switch via tftp, scp or sftp. Other port settings that should be valid cause the file transfer to abort with a "`corrupted download file`" error.
- **Port/Config (PR_1000778004) —** The switch accepts, via file transfer, a config file with invalid speed/duplex settings on dual-personality ports. Additionally, the 100-FX port settings do not survive a reboot.
- **TFTP/ACL (PR_1000771560) —** The **copy tftp command-file** command rejects ACL remarks if they do not contain the keywords **permit** or **deny**.
- **SNMPv3/Config (PR_1000777656) —** The SNMPv3 configuration is removed from the switch's config file after an update from K.12.xx to K.13.03.
- **SSH/Config (PR_1000777873) —** SSH becomes disabled (an ‘ip ssh’ entry in the config file becomes a ‘no ip ssh’ entry in the config file) after an update from K.12.xx to K.13.03.

  In K.12.xx software, SSH is disabled by default. In K.13.xx software, SSH is enabled by default. Since default values are not displayed in the output of **show run** or **show config** commands, this results in a difference in the configuration file output of SSH from K.12.xx to K.13.xx.
- **TFTP/Config (PR_0000000922) —** TFTP client configuration becomes disabled (‘`no tftp client`’) after an update from K.12.xx to K.13.03.
- **'show tech all/route'/Hang (PR_1000779458) —** When the **show tech all** or **show tech route** commands are used within a remote management session, the switch may hang.

- **Enhancement (PR_ 0000000081) —** The CLI **clear module** command allows you to remove module configuration information from the configuration file. For more information, see "Release K.13.04 Enhancements" on page 35.
- **Enhancement (PR_ 0000000082) —** The CLI **track interface** command allows you to configure tracking for a port or list of ports, or a trunk or list of trunks. For more information, see "Release K.13.04 Enhancements" on page 35.
- **Enhancement (PR_ 0000000084) —** DHCP Option 66 provides a way to automatically download and initially boot from a configuration that is different from the factory-shipped configuration. For more information, see "Release K.13.04 Enhancements" on page 35.
- **Enhancement (PR_ 0000000085) —** The DHCP relay address configuration enhancement provides a way to configure a gateway address for the DHCP relay agent to use for DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address. For more information, see "Release K.13.04 Enhancements" on page 35.
- **Enhancement (PR_ 0000000086) —** This enhancement allows rate-limiting of inbound broadcast and multicast traffic on the switch. For more information, see "Release K.13.04 Enhancements" on page 35.
- **Enhancement (PR_ 0000000087) —** This enhancement enables a Telnet client to use the hostname in command input. For more information, see "Release K.13.04 Enhancements" on page 35.
- **Enhancement (PR_ 0000000089) —** The CLI **show modules** command displays additional component information for system support modules and mini-GBICS. For more information, see "Release K.13.04 Enhancements" on page 35.
- **Enhancement (PR_ 0000000101) —** This enhancement adds a **vrrp** option to the **debug** command. For more information, see "Release K.13.04 Enhancements" on page 35.
- **Enhancement (PR_ 0000000420) —** This enhancement provides the **show tech** option for customizing **copy tftp** output. For more information, see "Release K.13.04 Enhancements" on page 35.
- **'show tech' (PR_0000000635) —** The **show tech** CLI command will cause an "`Invalid input: power`" error message to be displayed in the ProCurve Switch 6200yl-24G-mGBIC.
- **CLI (PR_0000000358) —** The output from the **show modules** CLI command shows the module serial number as being all zeros, or fails to show any output at all for that value.
- **CLI/sFlow (PR_0000000360) —** The switch administrator is unable to configure sFlow for ports on modules that have not been inserted yet into the switch.
- **CLI (PR_0000000476) —** Various CLI parameters are rejected by the switch as invalid when the administrator is trying to configure ports of transceivers/modules that have not yet been inserted into the switch. Affected commands include **ip source-binding**; **interface** `<x>` **power**; **interface** `<x>` **unknown-vlans block**; output from the command, **show vlans**; **interface** `<x>` **monitor**; and **mirror** `<x>` **port** `<x>`.

Release K.13.05

The following problems were resolved in release K.13.05 (not a public release).

- **Link/Config (PR_1000771549) —** On a ProCurve 3500yl Series Switch, a link will not come up after configuring the port mode from MDI to AUTOMDIX (on one side of the link).
- **Static Route/Config (PR_1000785177) —** The VLAN ID for the static route configuration is changed from its original value after updating from K.12.xx to K.13.03.
- **SNMP/Config (PR_1000780506) —** The TFTP transfer of a config file to the switch will fail if the config file contains the command **snmp-server trap-source** `<xx.xx.xx.xx>`.

- **Crash (PR_0000000971) —** Following MAC authentication of a number of users that have a RADIUS ACL, priority, and a number of other parameters applied, the switch may crash with a message similar to:

```
NMI event SW:IP=0x00334dc8 MSR:0x00029210 LR:0x00334e3c Task='mWebAuth' Task
ID=0x8413770. cr: 0x20004044 sp:0x08413260 xer:0x20000000
```

- **Crash (PR_1000783817) —** The switch may crash with a message similar to:

```
NMI event SW:IP=0x0010770c MSR:0x00029210 LR:0x00107714

Task='midmCtrl' Task ID=0x8417f00  cr: 0x24004084 sp:0x08417c08 xer:0x00000000
```

- **SNMP/Config (PR_1000786158) —** The TFTP transfer of a configuration file created on K.12.xx to a switch running K.13.03 will fail if the configuration file contains the command **snmp-server enable traps authentication**.
- **IPv6/Config (PR_1000781026) —** When a configuration file is transferred to the switch and the file contains a VLAN with the '`ipv6 mld`' statement, the switch alters the '`ipv6 mld`' statement to '`no ipv6 mld fastleave 1-A24,=1-Mesh,Trk1-Trk60,Dyn1-Dyn60`'.
- **SNTP/Config (PR_1000786156) —** The TFTP transfer of a configuration file created on K.12.xx to a switch running K.13.03 will fail if the configuration file contains the command **sntp server** `<x.x.x.x>`.
- **VLAN/Config (PR_1000782308) —** Updating from K.12.xx to K.13.03 may result in an incorrect port VLAN assignment.
- **Telnet-Server/Config (PR_0000000946) —** The TFTP transfer of a config file to the switch will fail if the config file contains the command **no telnet-server**.
- **Authorized-Manager/Config (PR_1000789930) —** The update from K.12.xx to K.13.03 does not translate the IP authorized-manager configuration properly.
- **UDLD (PR_0000001433) —** After the switch is rebooted, UDLD may continue to keep switch ports in a blocked state.
- **VLAN Mirroring/Config (PR_0000001240) —** The VLAN Mirroring configuration is changed from its original value after updating from K.12.xx to K.13.03.
- **Bootup/Flash (PR_1000785118) —** During the write-to-flash process, the OS file may become truncated if the switch is interrupted (by crash or power outage, for example). This fix minimizes that risk for ProCurve 3500yl, 6200yl, 5400zl Series Switches.
- **Bootup/Flash (PR_1000785113) —** During the write-to-flash process, the configuration file may become truncated if the switch is interrupted (by crash or power outage, for example). This fix minimizes that risk for ProCurve 3500yl, 6200yl, 5400zl Series switches.

Release K.13.06

The following problems were resolved in release K.13.06 (not a public release).

- **Static Route/Config (PR_0000001471) —** Rebooting a switch running K.13.03 may cause the static route configuration to become corrupted.
- **OSPF (PR_1000385566) —** When jumbo frames are enabled on a VLAN configured for OSPF, the state stops at EXCHANGE and EXSTART.
- **UDLD (PR_0000001616 and PR_0000001638) —** After the switch is rebooted, UDLD may continue to keep ports in a blocked state, particularly if the port is in a static LACP trunk.
- **CLI (PR_0000001643) —** The **ip authorized-managers** CLI command does not allow the 10.0.0.0 IP address to be used.

Release K.13.07

The following problems were resolved in release K.13.07 (not a public release).

- **Loopback Interface (PR_1000793862) —** A ping or Telnet session to a loopback address may fail intermittently. A traceroute to the loopback address completes successfully. This may cause some protocol packets to fail to reach the loopback address.
- **Crash (PR_0000001689) —** A switch running software version K.13.04 or higher may crash during configuration of a trunk group from either the CLI or menu interface. Event log messages may be similar to the following.

  ```
  W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone: 0x13000601
  ```

  ```
  W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone: 0x13000601
  W 03/11/06 03:18:53 00374 chassis: Ports 25-48: Lost Communications detected - Heart
  Beat Lost
  I 03/11/06 03:19:00 00375 chassis: Ports 25-48 Downloading
  I 03/11/06 03:19:01 00376 chassis: Ports 25-48 Download Complete
  I 03/11/06 03:19:15 00422 chassis: Ports 25-48 Ready
  ```

- **ARP Protect/Config (PR_0000001549) —** The VLAN ID range for the ARP protection configuration is changed from its original value after updating from K.12.xx to K.13.03.
- **Crash/Config Migration (PR_0000001607) —** If VRRP is configured on a switch and the switch is rolled back from K.13.xx to K.12.xx and then updated to K.13.xx again, the switch may get into a continuous crash/reboot state. The crash messages may be similar to the following.

  ```
  NMI event SW:IP=0x0015e960 MSR:0x00029210 LR:0x00229944 Task='mSess1' Task ID=x86fe5f0
  cr: 0x24022488 sp:0x086fd960 xer:0x00000000
  ```

  ```
  NMI event SW:IP=0x0083670c MSR:0x00029210 LR:0x007c4e1c Task='mIpCtrl' Task ID0x8c0ed90
  cr: 0x24004084 sp:0x08c0e4c0 xer:0x20000000
  ```

  ```
  Software exception at vrrp_common_lib.c:279 -- in 'swInitTask', task ID = 0x917630
  ```

  The fix involves partially removing some of the VRRP configuration and then generating an Event Log message similar to:

  ```
  E 07/14/06 10:14:15 00227 mgr: Partial config deleted for subsystem=vrrp; see release
  notes.
  ```

Release K.13.08

The following problems were resolved in release K.13.08.

- **SNMP/Config (PR_0000001672) —** The **snmp-server** configuration may change during the migration from K.12.xx to K.13.03.
- **Web/MAC Authentication (PR_1000793226) —** Web or MAC authentication to the switch by a client that moves from one port to another may either fail or cause the switch to crash with a message similar to the following.

  ```
  Program exception vector - Task='mWebAuth' Task ID=0x83bc390
  ```

Release K.13.09

The following problems were resolved in release K.13.09.

- **Crash (PR_0000001689a) —** A switch running software version K.13.04 or higher may crash during configuration of broadcast rate limiting. Event log messages may be similar to the following.

```
W03/11/0603:18:5300374chassis:Ports25-48SlaveROMTombstone:0x13000601
W03/11/0603:18:5300374chassis:Ports25-48SlaveROMTombstone:0x13000601W
03/11/06 03:18:53 00374 chassis: Ports 25-48: Lost Communications detected - Heart
Beat Lost I 03/11/06 03:19:00 00375 chassis: Ports 25-48 Down-
ading                                                                    I
03/11/06 03:19:01 00376 chassis: Ports 25-48 Download Complete
I 03/11/06 03:19:15 00422 chassis: Ports 25-48 Ready
```

- **Web Authentication (PR_0000002047) —** Use of Web authentication with MS-CHAP-v2 to Microsoft IAS may cause the switch to crash with a message similar to the following.

```
Software exception at exception.c:501 -- in 'mWebAuth', task ID = 0x8438440 Memory
System error at 0x7f56610 - memPartFree
```

- **MAC Authentication (PR_0000002075) —** A client that fails MAC authentication will be blocked by AAA rather than the port being moved, unblocked, into a configured Unauthenticated VLAN.

Release K.13.10

The following problems were resolved in release K.13.10 (never released).

- **VLAN/Config (PR_1000782308)** — Updating from K.12.xx to K.13.03 may result in an incorrect port VLAN assignment.
- **MAC Authentication (0000002318)** — Authenticated MAC Auth clients may intermittently get placed into the unauthenticated VLAN and never come on-line.
- **Port Security (PR_1000777162)** — When Port Security is configured for static MAC address learning, prolonged flooding of unicast traffic may occur under certain conditions.
- **Static Routes/Config (0000001461)** — Static routes mapped to VLANs are incorrectly migrated during the update from K.12.xx to K.13.xx.
- **Wrong Error Message/VRRP (0000000909)** — You may receive an "inconsistent value" error message when attempting to add (max+1) entity for VRRP to track. The correct error message should be "too many entries to track."
- **RADIUS/Jumbo (PR_ 1000779048)** — When an 802.1X-enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **RADIUS (0000001164)** — The switch drops RADIUS messages with EAP-packets larger than 1496 bytes.
- **Auto-TFTP/Config (PR_0000001410)** — The Auto-TFTP configuration is lost during the update from K.12.xx to K.13.03.

Release K.13.11

The following problems were resolved in release K.13.11 (not a public release).

- **TACACS+ (PR_1000764992)** — After authentication to the switch using TACACS+, the switch may crash with a message similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:.Stack Frame=0x08632568 HW
Addr=0x30313165 IP=0x008bba1c Task='mTacacsR' Task ID=0x86329c0.fp: 0x08632750
sp:0x08632628 lr:0x008bba00
```

- **DHCP Snooping (PR_1000469934)** — When DHCP Snooping is enabled and configured, and a client sends a "DHCPINFORM" after receiving address information, the DHCP server response is not forwarded to the client by the switch.
- **Crash (1000790369)** — Use of VRRP may cause the switch to crash with a message similar to the following.

```
Software exception at vrrp_common_lib.c:313 -- in 'mVrrpCtrl', task ID = 0x8526e20
```

- **Static Route (0000002610)** — After an update/roll-back/update (K.12 to K.13 to K.12 to K.13), static route entries may become corrupted, causing the CLI to hang following execution of the **show ip route** command.

Release K.13.12

The following problems were resolved in release K.13.12 (never released).

- **Crash (PR_0000002347)** — When a VLAN is deleted, all the modules may crash with a message similar to the following.

```
ipamSRtDescr.c Line:289 mIpAdMUpCt0x4484364c ->ASSERT:  failed
```

- **Certificate (PR_1000416167)** — The Web Management interface submission form limits CA-signed certificates to 1800 bytes.
- **802.1X (PR_0000002036)** — 802.1X with Funk Steel Belted RADIUS server causes the switch to fail to assign the VLAN that it was sent with the "Tunnel-Private-Group-Id" parameter.
- **Module Selftest (PR 0000001273)** — After a reboot, ports 1-24 or ports 25-48 on the ProCurve 3500yl, or ports 1-24 on the 6200yl switches, may become unresponsive followed by green and amber port LEDs remaining lit. The ports recover automatically. The log file will show the following messages.

```
chassis: Ports 1-24: Slave ROM Tombstone: 0x13000601
chassis: Ports 1-24: Lost Communications detected - Heart Beat Lost(4A)
chassis: Ports 1-24 Downloading
chassis: Ports 1-24 Download Complete
chassis: Ports 1-24 Ready
```

SNMP (PR_1000772026) — The wrong OID is set for a redundant power supply (RPS) failure.

- **CLI (PR_0000002177)** — When a ProCurve switch yl 10-GbE module (J8694A) is inserted into a 3500yl or 6200yl switch, the switch may prompt, "Do you want to save the config?," even when no changes to the config have been made.
- **Loopback Interface (PR_0000002165)** — A ping or Telnet session to a loopback address may fail intermittently. A traceroute to the loopback address completes successfully. This may cause some protocol packets to fail to reach the loopback address.
- **CLI (PR_1000745509)** — Output from the CLI command **show ipv6 neighbors vlan** <x> is not displaying the correct age, and it may erroneously display the State Age as "stale" after a recent learn.

- **ICMP (PR_1000764033)** — ICMP TTL expired messages are being sent with a source address of the interface from which the message is sent rather than the from the interface that receives the expired packet.
- **Web (PR_1000761014)** — The Web interface truncates 16 character passwords to 15 characters.
- **MIB (PR_1000770084)** — Several OIDs in MIB violate RFC 2737 and RFC 4133. The affected OIDs are:

```
 .iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalT-
able.entPhysicalEntry.entPhysicalHardwareRev
  .iso.org.dod.internet.mgmt.mib-
2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhys calEntry.entPhysical-
FirmwareRev
  .iso.org.dod.internet.mgmt.mib-
2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhys calEntry.entPhysical-
SerialNum
  .iso.org.dod.internet.mgmt.mib-
2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhys calEntry.entPhysi-
calModelName
```

Release K.13.13

The following problems were resolved in release K.13.13 (never released).

- **802.1X (PR_1000446227)** — Switch 802.1X authentication running over PAP does not work if the RADIUS message authenticator attribute is required. This fix added the message authenticator attribute to non-EAP RADIUS responses.
- **VLAN/MSTP (PR_0000002103)** — The alteration of the VLAN/MSTP instance mapping in the pending configuration is not properly functioning. Any attempt to remove a single VLAN ID (VID) from one MSTP instance and then assign it to another MSTP instance fails, though specifying a VID range succeeds.
- **SSH (PR_0000001296)** — Upon reboot, if no key is present, a 1024-bit dsa ssh host key is installed rather than the previous default host key type of a 2048-bit rsa key.
- **CLI (PR_1000430534)** — Output from the show port-access mac-based CLI command may omit connected clients.
- **Static Routes/Config (0000001461)** — Static routes mapped to VLANs are incorrectly migrated during the update from K.12.xx to K.13.xx. This is a further improvement to the fix originally implemented in K.13.10.
- **DHCP (PR_0000002888)** — A client may not be able to get a DHCP address when the Management VLAN is configured on the switch.

Release K.13.14

The following problems were resolved in release K.13.14 (not a public release).

- **OSPF (PR_0000003395)** — If a transceiver or mini-GBIC is inserted (hotswapped) on a port that is a member of a VLAN configured for jumbo frames and OSPF, the OSPF state stops at EXCHANGE and EXSTART.

Release K.13.16

The following problems were resolved in release K.13.16 (not a public release).

- **Enhancement (PR_0000001641)** — This enhancement allows the user to set the console inactivity time out without reboot. For more information, see “Release K.13.16 Enhancements” on page 35.

- **Enhancement (PR_1000780247)** — This enhancement provides hpicf Download MIB support for transferring configuration files both to and from a TFTP server. Prior to this enhancement, MIB support was limited to downloading and uploading software files. For more information, see "Release K.13.16 Enhancements" on page 35.
- **Enhancement (PR_0000001430)** — This enhancement allows the user to configure access methods for IP Authorized Manager entries. For more information, see "Release K.13.16 Enhancements" on page 35.
- **Enhancement (PR_0000000090)** — This enhancement allows you to choose which information to display when you enter the **show interfaces** command. For more information, see "Release K.13.16 Enhancements" on page 35.
- **Enhancement (PR_0000000857)** — This enhancement reduces the PIM delay time, thereby reducing the amount of time it takes for a packet to arrive at its destination when an IGMP Join is issued. For more information, see "Release K.13.16 Enhancements" on page 35.
- **Enhancement (PR_0000001790)** — This enhancement provides the **no-tag-added** parameter that gives the user the option of not tagging a mirrored copy of an outbound packet. For more information, see "Release K.13.16 Enhancements" on page 35.
- **Enhancement (PR_1000756562)** — This enhancement provides concurrent Web/MAC and 802.1x authentication. For more information, see "Release K.13.16 Enhancements" on page 35.
- **Enhancement (PR_0000000088)** — This enhancement provides new features for use with SSH. The SSH enhancements are: AES encryption (included in the K.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection; A configurable key; Message Authentication Code (MAC) configuration. A new configuration option provides the ability to configure which MACs a client is permitted to use; Feedback information; and, SSH CLI **show** command information enhancements. For more information, see "Release K.13.16 Enhancements" on page 35.
- **Config (PR_0000000741)** — When the rate limit for broadcast or multicast inbound is set to 0% (i.e. blocking all traffic), output from the CLI command show running config doesn't display any rate limit information. If the rate limit is set to 100% (i.e. allow all traffic – the default), show running config shows that rate-limiting is set to 100%. The correct behavior is for non-default values to be displayed in the configuration.

Release K.13.17

The following problems were resolved in release K.13.17 (not a public release).

- **RADIUS/Jumbo (PR_ 1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **Protocol Starvation (PR_0000003814)** — If the switch is configured for routing, certain packets may cause a packet buffer leak, resulting in some or all of the following symptoms:
  - OSPF neighbor relationships and route information are lost
  - PIM neighbor relationships are lost
  - Telnet, Ping, and SNMP become unresponsive

  Authorized Managers (PR_1000806039) — ProCurve Manager may delete Authorized Managers that have been configured on the switch.
- **Crash (PR_0000001756)** — Configuration of VLANs and VLAN port assignment using SNMP may cause the switch may crash with a message similar to the following.

```
Software exception at bcmHwVlans.c:149 -- in 'mAdMgrCtrl', task ID = 0x18636e8 -> ASIC
call failed: Entry not found.
```

- **Crash (PR_1000715077)** — When RADIUS Accounting is configured, the switch may crash with a message similar to the following.

  ```
  NMI event SW:IP=0x002bd6c4 MSR:0x00029210 LR:0x002bc6a8 Task='mAcctCtrl' Task
  ID=0x85e9f10 cr: 0x48000084 sp:0x085e9e38 xer:0x20000000
  ```

- **Static Route/Config (PR_0000003962)** — Updating from K.13.03 - K.13.09 to K.13.10 - K.13.16 can cause static routes configured with a VLAN as the next hop (vs. an IP address) do not translate correctly.

- **SNMP (PR_1000761379)** — When an SNMP get is used to gather statistics, the interface B1 on a J8702A module only updates its SNMP counters on every other query.

- **SNMP (PR_0000001807)** — Use of a correctly configured third party utility to connect to the switch via SNMPv3 may result in the following event log message.

  ```
  SNMP Security access violation from <ip address>
  ```

- **PIM/Config (PR_0000002040)** — PIM configurations mapped to VLANs are incorrectly mapped after updating from K.12.xx to K.13.xx. Note that while this fix addresses the way the configuration is updated, rolling back the software while using the same configuration can still result in corruption in PIM configurations mapped to VLANs.

Release K.13.18

The following problems were resolved in release K.13.18 (never released).

- **UDLD (PR_0000002473)** — UDLD protocol packets received on a (non-UDLD) trunk port are incorrectly forwarded out of same port they are received on, resulting in high CPU usage on the switch.

- **Enhancement (PR_1000406763)** — New commands were added to the CLI response to the "show tech" command. For more information, see “Release K.13.18 Enhancements” on page 39.

- **SSH (PR_0000002946)** — ProCurve 8212zl switches do not automatically create the SSH folder on /cfa0; the result is that attempts to generate a crypto key may result in the following error.

  ```
  Installing new RSA key.  If the key/entropy cache is depleted, this could take up to
  a minute.
  Operation aborted.
  ```

- **ACL (PR_0000004860)** — Mirrored ACL packets that match deny statements, are mirrored; the correct behavior is that only packets matching permit statements should be mirrored.

- **Crash (PR_0000004166)** — When the PIM Sparse Mode "trap all" parameter is configured and the link to PIM neighbor is disabled, the switch will crash and may report a message similar to the following.

  ```
  Software exception at exception.c:501 -- in 'mPimsmCtrl', task ID = 0x8215d30 Memory
  system error at 0x7c838f0 – memPartFree
  ```

- **Mirror/CLI (PR_0000003269)** — The CLI incorrectly configures the option "no-tag-added" across multiple mirror sessions, resulting in the wrong output saved to the config file.

- **Wake-On-LAN (PR_0000004794)** — Wake-On-LAN does not always work successfully.

- **IP Phone (PR_0000004803)** — A tandem IP phone may stop talking to the switch after a connected PC login failure and reboot.

- **PIM-SM (PR_0000005219)** — When the switch sends a “Register-Stop” message, it will use an incorrect source IP address in the packet header of the message. Rather than using the IP address configured for the PIM RP, the switch uses the VLAN IP address.

- **Mirroring (PR_0000002926)** — When mirroring on a mesh or trunk port, the mirror session is not cleared after the mesh or trunk configuration is deleted.

Release K.13.19

The following problems were resolved in release K.13.19 (not a public release).

- **Enhancement (PR_0000003808)** — This enhancement allows the user to create command aliases for use in place of command names and their options. For more information, see "Release K.13.19 Enhancements" on page 39.
- **Enhancement (PR_0000000818)** — This enhancement allows the user to enter addresses and filter parameters for syslog using SNMP, which allows more options for remote access and management of the switch. For more information, see "Release K.13.19 Enhancements" on page 39.
- **Enhancement (PR_0000003390)** — This enhancement allows the user to customize Web Authentication HTML pages. For more information, see "Release K.13.19 Enhancements" on page 39.
- **Enhancement (PR_1000460265)** — This enhancement provides the user with Dynamic IP Lockdown, which is used to prevent IP source address spoofing on a per-port and per-VLAN basis. For more information, see "Release K.13.19 Enhancements" on page 39.

Release K.13.20

The following problems were resolved in release K.13.20 (not a public release).

- **Enhancement (PR_0000004124)** — Support was added for the J9144A ProCurve 10-GbE X2-SC LRM Optic. For more information, see "Release K.13.20 Enhancements" on page 40.
- **10-GbE (PR_0000001701)** — Sometimes, the LRM optic is misidentified as an LR optic.
- **CLI (PR_0000001528)** — 10-GbE X2 transceivers do not report their part numbers in response to the CLI command **show tech transceivers**.
- **X2 Transceivers (PR_0000004758)** — Some ProCurve SR and ER X2-10GbE (J8436A, J8437A) transceivers have a timing issue that prevents the transceivers from being correctly identified either when hot swapped or during a cold boot.
- **LEDs (PR_0000005623)** — Upon insertion of a removable transceiver – either X2 or SFP - the link LED fails to light for the 2 second-long indication of insertion confirmation.
- **Event Log (PR_0000005624)** — A failed "removable" transceiver results in two event log messages rather than just one.
- **Authentication (PR_0000005582)** — Sometimes PC in the PC-phone tandem authentication does not get authorized on its untagged VLAN.

Release K.13.21

The following problems were resolved in release K.13.21 (never released).

- **CLI (PR_1000760929)** — Output from the CLI command **show name int <***port list***>** fails to display the port number for interfaces with numbers larger than 9.
- **Config (PR_0000003638)** — Fastboot can be configured, but then it cannot be disabled.

- **Multicast Filter (PR_0000002988)** — Multicast filters may become corrupted following their initial configuration, save and subsequent switch reload.
- **Self-Test (PR_0000001406)** — The failure of a single module within a Switch 8212zl or 5400zl chassis may cause false self-test failures for other installed modules.
- **CLI (PR_0000005300)** — The displayed output of the CLI command **show ip pim rp-set** is not properly formatted.
- **CLI (PR_0000005302)** — The displayed output of the CLI command **show ip pim pending** is not properly formatted.
- **CLI (PR_1000782972)** — An incorrect line voltage value may be displayed in the output of the **show system power** CLI command.
- **CLI (PR_0000005381)** — Attempts to perform a **copy flash <primary|secondary>** at the CLI of a 8212zl switch running K.13.05 or higher will fail with the following error.

```
Flash-to-flash copy of product code failed
```

- **Config (PR_1000781011)** — Copying a config onto a switch allows the appearance of an invalid flow control setting (enabled) on half duplex ports.
- **Config (PR_1000781015)** — When the MDIX-mode is configured for dual-personality ports, copying a config onto a switch fails and produces a message about config file corruption.
- **Config (PR_1000781031)** — When the valid port setting 'auto-1000' is configured for any 10/100/1000 interface in an external configuration file and the configuration file is copied to the switch, the system returns the port setting to the default value, changing 'auto-1000' to 'auto.'
- **CLI (PR_0000004687)** — The CLI command **ip access-list resequence <name-str>** does not accept a number for the ACL title as it should.
- **PIM-SM (PR_0000006180)** — PIM Sparse Mode may choose an incorrect rendezvous point (RP), causing interoperability problems. This fix changes the way a RP is chosen such that ALL the devices running "K" versions of software must be on either pre- or post-fix software version in order to use the same criteria to choose the PIM RP.
- **Event Log (PR_1000755803)** — ProCurve Manager is unable to display a link to the switch Web Interface in events generated by Fault Finder.

Release K.13.22

The following problems were resolved in release K.13.22 (not a public release).

- **CLI (PR_0000002856/1000769143)** — The switch is unable to execute the CLI command **show tech** while in QinQ svlan mode.
- **OSPF (PR_0000006183)** — OSPF ECMP may drop up to 50% of the traffic destined for its next hop.
- **Mini-GBIC (PR_0000006298)** — Mini-GBICs in dual-personality ports fail self-test when the switch is running K.13.20-K.13.21. Workaround: Configure fastboot.
- **Licensing (PR_0000006554)** — An invalid hardware ID (required for Premium Licensing in 3500yl and 5400zl switches) is created by switches running K.13.15 - K.13.21.

Release K.13.23

The following problems were resolved in release K.13.23.

- **Crash (PR_0000006624)** — When using the Web Management Interface on software version K.13.17 and higher, the switch may crash if the "Configuration" and then "IP Configuration" tabs are clicked. There may be other triggers for this crash. The switch will display a message similar to the following.

```
      PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x0815da48 HW
Addr=0xa2d3e193 IP=0x00169178
      Task='tHttpd' Task ID=0x fp: 0x00a650c4 sp:
```

- **Authentication (PR_0000007209)** — A PC behind a tandem IP phone is not able to authenticate.

Release K.13.24

The following problems were resolved in release K.13.24 (not a public release).

- **OSPF (PR_0000006183a)** — OSPF ECMP may drop up to 50% of the traffic destined for its next hop. This fix adds to that implemented in K.13.22 via the same PR.
- **Crash (PR_0000003949)** — Implementation of OSPF ECMP route changes may cause the switch to crash with a message similar to the following.

```
Software exception at exception.c:501 -- in 'eRouteCtrl', task ID = 0x83da3f0 -> Memory
system error at 0x7bd9540 - memPartFree
```

- **802.1X (PR_ 0000007259)** — Configuring 802.1X without activating it does not function as expected, resulting in blocking of the port.

Release K.13.25

The following problems were resolved in release K.13.25.

- **SSH (PR_0000002934)** — Copying the client's public SSH keys from the switch fails with the following error.

```
Couldn't read from remote file "/ssh/mgr_keys/authorized_keys
```

- **Crash (PR_0000004023)** — Repeated PCM configuration scans may cause the switch to crash with a message similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x07af44c0
HW Addr=0x6520463a IP=0x00965a88 Task='tSsh0' Task ID=0x7af4810fp: 0x013d97cc sp:0
```

- **Management Module (PR_0000005902)** — The management module may become unresponsive, resulting in loss of Telnet, Web Management, and console access functionality of the switch.
- **802.1X Authentication (PR_0000002695)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. This allows the RADIUS server to reply with a large fragment which the switch does not process, causing the authentication to fail. This is an additional fix for the issue described in K.13.17 via PR_1000779048.
- **GVRP/RADIUS (PR_0000006051)** — RADIUS-assigned VLANs are not propagated correctly in GVRP. Please see "Note: This fix is associated with some new switch behavior:" for a description of the behavior change with this fix.

  Note: This fix is associated with some new switch behavior:

When only one port has learned of a dynamic VLAN, it will advertise that VLAN if an auth port has been RADIUS-assigned that dynamic VLAN, regardless of the unknown-VLANs configuration of that port. The fix accommodates RADIUS-assigned (and hpicfUsrProf MIB-assigned) tagged VLANs as well as untagged VLANs. These changes are enabled by default and are not configurable. This fix does not modify any other GVRP behavior.

- **Assert (PR_0000001836)** — VRRP configuration conversion from K.12.xx to K.13.xx software may experience a crash (assert) in ConfigRecIndex().
- **Assert (PR_0000005208)** — Entering **no ipv6 enable** at the CLI may result in a crash with a message similar to the following.

```
Software exception at ConfigRecIndex.cc:421 -- in 'mSess1', task ID = 0x58c1c38->
ASSERT:  failed.
```

- **Config (PR_0000002620)** — A MAC-lockdown command that includes VLAN information may fail when it is copied to the default configuration.

Release K.13.26 through K.13.39

Software never built.

Release K.13.40

The following problems were resolved in release K.13.40 (Never released).

- **Enhancement (PR_0000003127)** — Link Trap and LACP Global Enable/Disable. For more information, see "Release K.13.40 Enhancements" on page 40.
- **Enhancement (PR_0000003128)** — The ability to clear statistics was added. For more information, see "Release K.13.40 Enhancements" on page 40.
- **Enhancement (PR_0000003718)** — The MAC Lockout limit was increased. For more information, see "Release K.13.40 Enhancements" on page 40.
- **Enhancement (PR_0000007388)** — Crash Log Debug. For more information, see "Release K.13.40 Enhancements" on page 40.
- **Crash (PR_0000003597)** — Configuring a kbps based rate-limit on 10Gig port may trigger a crash in the area of `bttfHwRateLimits.c:2191`.

Release K.13.41

The following problems were resolved in release K.13.41 (Not a public release).

- **AAA (PR_0000008409)** — The CLI commands **aaa authentication** and **aaa accounting** return a `resource unavailable` error.
- **PCM (PR_0000008113)** — Repeated ProCurve Manager Config Scans may trigger subsequent Config Scan failure.

Release K.13.42

The following problems were resolved in release K.13.42 (Never released).

- **Config (PR_0000007953)** — The config line **spanning-tree instance <n> vlan <vid>** is truncated in some cases, causing loss of configuration after reload of the config file.

- **CLI (PR_0000000912)** — The CLI command **copy tftp show-tech** fails, resulting in failure to create a custom show-tech file on the switch.
- **TFTP (PR_0000008559)** — The switch administrator is unable to download a new image file after executing the CLI command **erase primary flash**; a `corrupted download file` error is reported.
- **ARP (PR_0000008011)** — When port-security is configured, the switch sends ARP requests twice for an unknown DA, making the switch appear to be slow.
- **SFTP/SCP (PR_0000008270)** — Beginning with software version K.13.25, SFTP/SCP will not close the "client" session after the file transfer. The client session will need to be manually closed.
- **RADIUS (PR_0000007278)** — MAC-based authentication doesn't work with a secondary RADIUS server unless the primary and secondary RADIUS server keys are identically configured.
- **Crash (PR_0000006476)** — Some configuration commands entered at the CLI (e.g. **web**, or **no web**) may cause the switch to crash with a message similar to the following:

  ```
  PPC Data Storage (Bus Error) exception vector 0x300:Stack Frame=0x088befe8HW
  Addr=0x00cff108 IP=0x0096ca4c Task='mSnmpCtrl' Task ID=0x88bf320 fp: 0x0845a7e0
  ```

- **Crash (PR_0000005940)** — An attempt at tab completion for some configuration tasks in the PIM context may cause the switch to crash with a message similar to the following:

  ```
  Software exception at parser.c:6291 -- in 'mSess1', task ID = 0x82ab3b0
  ```

- **CLI (PR_0000004042)** — The CLI command **snmp-server response-source dst-ip-of-request** does not work as expected when the destination IP address of the *SNMP Request* is the Loopback IP. The source IP address of the *SNMP Response* should be the destination IP of the *SNMP Request*, but instead the switch uses the IP address of the active interface from which the *SNMP Response* was sent.
- **CLI (PR_0000007686)** — The switch does not allow IP authorized-manager configuration of 10.0.0.0.
- **TACACS+ (PR_0000003839)** — The TACACS server configuration parameter accepts an address from an invalid/reserved IP range: 0.0.0.1 to 0.255.255.255.
- **Boot Log (PR_0000009434)** — The switch doesn't create an event log message after deleting an invalid TACACS server host config entry upon bootup following an update from K.12.xx to K.13.xx

Release K.13.43

The following problems were resolved in release K.13.43 (Not a public release).

- **CLI (PR_0000005759)** — There may be odd CLI output in response to a **show modules** command, if that command is executed during module initialization.
- **SNMP (PR_0000001926)** — An SNMP query for the MIB **ifInUnknownProtos** returns incorrect and varying results.
- **Enhancement (PR_0000003557)** — The ability to enable/disable the USB port via CLI and SNMP was added. Note that after being disabled and subsequently re-enabled, the USB port may not function consistently with the PCM USB Autorun features until the switch has been reloaded. For more information, see "Release K.13.43 Enhancements" on page 42.

Release K.13.44

The following problems were resolved in release K.13.44 (Not a public release).

- **ICMP Redirects (PR_0000004534)** — With the next hop router is in the same VLAN as the host machine, the switch does not generate ICMP redirects.
- **Crash (PR_0000009736)** — In some situations, ICMP redirects may cause the switch to crash with a message similar to the following.

  ```
  PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x084f2e40
  HW Addr=0x00cff108 IP=0x00870e5c Task='mIpPktRecv' Task ID=0x84f3140 fp: 0x0a84d994
  ```

- **CLI (PR_1000803731)** — If the "|" character exists in the banner text of a configuration file downloaded via TFTP transfer, the banner text may become corrupted, or the TFTP transfer may fail with a `corrupted download file` error message.
- **Hang (PR_0000007806)** — Using the CLI command **no arp** on ARP entries that do not exist may cause the switch to hang.
- **CLI (PR_0000008617)** — The **copy** command for USB options has incorrect optional parameters for plain text files.
- **RADIUS Accounting (PR_0000004139)** — Procurve switches do not send the accounting-request to a RADIUS server upon execution of the **reload** CLI command.
- **RADIUS Accounting (PR_0000004145)** — An incomplete "Calling-Station-ID" field is sent in the accounting-request to the RADIUS server upon execution of the **boot system** CLI command.
- **RADIUS Accounting (PR_0000004141)** — The "Acct-Status-Type" attribute is missing in the accounting-request to RADIUS server upon execution of the **boot system** CLI command.
- **Terminal Display** (PR_0000008238) — The default boot message is displayed with the wrong formatting if the terminal width is changed.
- **CLI (PR_0000008236)** — The **enable** CLI command is listed in enable-mode help.
- **UDLD (PR_0000009505)** — UDLD misconfiguration (where UDLD is enabled on one side and disabled on the other) could lead to a unicast packet storm which results in MSTP is running with multiple roots.
- **CLI (PR_0000008217)** — The **copy flash** CLI command does not allow the user to specify a source OS location (primary/secondary).

Release K.13.45

The following problems were resolved in release K.13.45.

- **STP (PR_0000010815)** — When a switch configured with BPDU protection is added to a network, if the MSTP configuration of the uplink port is changed from **auto-edge** to **no auto-edge** there is a topology change event that takes place as the switch asserts itself as a new root.
- **Enhancement (PR_0000010783)** — Support was added for the following products.

  J9099B - ProCurve 100-BX-D SFP-LC Transceiver

  J9100B - ProCurve 100-BX-U SFP-LC Transceiver

  J9142B - ProCurve 1000-BX-D SFP-LC Mini-GBIC

  J9143B – ProCurve 1000-BX-U SFP-LC Mini-GBIC

  For more information, see "Release K.13.45 Enhancements" on page 43.

- **Transceivers (PR_0000010525) —** Intermittent self test failure may occur if transceivers are hot-swapped in and out of the switch in too short a time frame. Note that even with this fix, transceivers should always be allowed to initialize fully prior to removal and subsequent re-insertion.

  Best Practice Tip: Upon hot insertion of a transceiver, the Mode LED will come on for two seconds while the transceiver is initialized. Once the Mode LED has extinguished, it is safe to remove the transceiver.

- **Selftest Failure (PR_0000010937)** — Rarely, the switch may experience self test failure of all the modules. Messages like the following will be visible in the event log. Re-seating the modules may allow successful self-test to occur.

  ```
  W <date/time stamp> 00374 chassis: Slot # Failed to boot-timeout-(SELFTEST)
  ```

Release K.13.46

The following problems were resolved in release K.13.46. (Never released.)

- **sFlow (PR_0000003723)** — The switch uses the loopback as the sFlow agent address, even after explicit configuration of the VLAN IP address and the collector receiving the sFlow packets.

- **SCP/SFTP (PR_0000009174)** — Failure to upload a configuration via SFTP/SCP may occur. As a result, it is possible that the switch may become unresponsive or crash with a message similar to the following.

  ```
  Software exception at cfg_edit.cc:313 – in ‘swinitTask’, task ID = 0xa9bbcc0
  ```

- **SCP (PR_0000011488)** — The switch does not return the scp/sftp session after new software is uploaded.

- **CLI (PR_0000009997)** — The CLI response to the **boot set-default flash <primary | secondary>** configuration setting is inconsistent between the zl (5400zl/8212zl) and yl (3500yl/6200yl) switches, potentially causing issues for customers running scripts.

- **Password Encryption (PR_0000011828)** — The Password Manager portion of the Include Credentials feature is using SHA-0 Instead of SHA-1 for creation of the hash value. In order to accommodate customers that have worked around this issue, this fix will translate the configuration and correctly report the use of SHA-0 in the config after a software update containing this fix.

  Example line from password encryption config prior to the fix:

  ```
  password operator sha-1 "lsadkjlkjfsd..."
  ```

  Example of what that line might look like after the fix:

  ```
  password operator sha0 "lsadkjlkjfsd..."
  ```

  No switch administrator intervention is required for the forward configuration translation to occur.

  Support Note: This fix has implications for rolling back the software. If password encryption is configured and a switch running software with the fix is rolled back to a software version prior to the fix using the same config file, the config loading will fail, and error messages for each line containing "sha0" or "sha1" will be displayed on the switch terminal. In the following example, sha1 was line 14 in the config, and sha0 was on line 15 of the config.

  ```
  Line:14. Invalid input: *sha1*
  Line:15. Invalid input: *sha0*
  ```

  To avoid configuration compatibility issues, please follow the instructions in the “Best Practices for Major Software Updates” on page 5. If roll back to a pre-fix software version occurs without following the Best Practice suggestion (association of a compatible config file with a software version), the switch administrator should gain access to the switch by hitting <enter> at the password prompt, and must then reconfigure the password encryption with valid parameters (the pre-fix CLI syntax is **SHA-1,** versus the post-fix CLI use of **SHA0** or **SHA1**).

  The default hash value for newly configured password encryption on a software version with this fix is **SHA1**.

- **CLI (PR_0000009860)** — Output from the CLI command **show module** erroneously reports the 8212zl System Support Module (SSM) product number as J8784A instead of J9095A.
- **Crash (PR_0000011049**) — Copying a configuration with mirroring enabled from USB to switch may trigger a software exception with a message similar to the following.

```
Software exception at cli_mirror.c:9953 -- in 'mftTask', task ID   = 0xa932bc0
```

- **VRRP (PR_0000003634)** — When the VRRP Owner router (with preempt-delay-time configured) is rebooting, the VRRP Backup router momentarily gives up Master role (but does resume it) before the VRRP Owner is back online. This may cause an unexpected outage.
- **DHCP Relay (PR_0000011726)** — When the VRRP backup router is the master for the network, DHCP Discover packets are relayed with a corrupted IP address for the Relay Agent. This causes the server to look up a client address range for an invalid network segment, and ultimately fail to communicate with the DHCP Server.
- **PC/Phone Authentication (PR_0000010104)** — When using an IP phone in tandem with a PC, sometimes the post-authentication VLAN assignment of the PC is delayed.

Release K.13.47

The following problems were resolved in release K.13.47. (Never released.)

- **OSPF ECMP (PR_0000004798)** — Some IP subnets which are multiple hops away are not reachable from certain clients despite the presence of the target subnet in the switch routing table. Workaround: Initiate a traceroute from the switch to the client PC.

Release K.13.48

The following problems were resolved in release K.13.48. (Never released.)

- **DHCP Relay (PR_0000013661/000008196)** — After adding a second IP Address to a VLAN with IP Helper configured, the switch Relay Agent IP Address gets corrupted such that the DHCP server does not recognize the request as part of a configured scope, and drops the request. Workaround: Save the configuration and reload the switch after configuration of an IP Helper address and DHCP Relay.
- **Module/Fabric Errors (PR_0000012418)** — Switches running system software version K.12.45 or higher may see one or more of the following errors in the event log, potentially causing false self-test failures.

```
W 12/02/08 14:24:59 00374 chassis: HSL Non-Fatal F0: SLOT D HSL     #11 - HSL status
FF002000                                                              W 12/02/
08 14:25:25 00374 chassis: Slot D: Msg loss detected - no ack for seq # 37
W 12/02/08 14:25:38 00374 chassis: Slot D Slave ROM Tombstone:  0x13000601
W 12/02/08 14:25:38 00374 chassis: Slot D: Lost Communications  detected – Source
Message System(59)
W 12/02/08 14:25:58 00374 chassis: HSL Non-Fatal F0: SLOT D HSL   #11 - HSL status
FF002000 W 12/02/08 14:26:17 00374 chassis: Slot D: Msg loss detected - no       ack
for seq # 40                                              W 12/02/08 14:27:28 00374
chassis: Slot D Failed to boot-timeout-     (SELFTEST)
```

- **OSPF ECMP (PR_0000013777)** — When the switch is acting as an ECMP router with multiple next hops available, sometimes it fails to route packets received on a local VLAN to hosts that are reachable via ECMP routes. The result is intermittent connectivity to hosts on the other side of ECMP routes.
- **Boot ROM (PR_0000014318)** — This build introduces the new K.12.14 boot ROM, a prerequisite for future updates. Please do not interrupt power to the switch during the software/boot ROM update!

Release K.13.49

The following problems were resolved in release K.13.49.

- **Auto-TFTP (PR_0000014646/0000013552)** — Certain software file names may trigger auto-tftp to reload the same software file repeatedly.

Release K.13.50

Software never released.

Release K.13.51

The following problems were resolved in release K.13.51.

- **Enhancement (PR_0000003144)** — Support is added for multiple RADIUS groups. For more information, see "Release K.13.51 Enhancements" on page 44.
- **Enhancement (PR_0000003141)** — Support is added for SSH Secure to RADIUS authentication. For more information, see "Release K.13.51 Enhancements" on page 44.
- **Enhancement (PR_0000000083)** — Support is added for a MAC-Auth failure HTTP Redirect option. For more information, see "Release K.13.51 Enhancements" on page 44.
- **Enhancement** – Support is added for the J9154A HP ProCurve ONE Services zl Module. For more information, see "Release K.13.51 Enhancements" on page 44.
- **Services Module (PR_0000010902)** — When the switch communicates through the ports that are connected to the HP ProCurve ONE zl Services Module, it could transmit layer 2 frames using the same source MAC address as being used by the Services module itself. This could potentially cause confusion to the application running on the Services module. This fix alters the mechanism for assignment of MAC addresses of the HP ProCurve ONE Services zl module to make them unique. As a result, an application running on the module prior to this fix may communicate using a different MAC address than it does after this fix.
- **Services Module (PR_0000010463)** — There is a brief period in which output from the CLI command **show services** indicates that it is safe to remove the module before the module has fully halted.
- **Services Module (PR_0000008101)** — Changes were made in the switch software to improve the ONE Services zl Module boot process.

Release K.13.52

The following problems were resolved in release K.13.52. (Not a public release.)

- **Config (PR_0000014381)** — Switches running K.13.21 or newer software may be unable to upload a valid config file to the switch, if it is set with the parameter, speed-duplex 1000-full, and on a dual personality port with a mini-GBIC inserted. The switch will display a message similar to the following. (The example below contained the speed-duplex value in line 8 of the config, and the value was applied to port 47.)

```
line: 8. Value 1000-full is not applicable to port 47.
Corrupted download file.
```

- **Self Test (PR_0000009650)** — In some cases, when a bank of ports fails on the yl switches, the failure status is not appropriately recognized and reported in the switch's event log.

- **Enhancement (PR_0000013786)** — Support is added for source IP identification. For more information, see "Release K.13.52 Enhancements" on page 53.
- **Enhancement (PR_0000008243)** — Support is added for an eavesdrop prevention option. For more information, see "Release K.13.52 Enhancements" on page 53.
- **Config (PR_0000012917)** — Attempts to upload a config will fail if the configuration contains valid configuration lines involving fixed MAC addresses and static learn mode. For example, this type of parameter in line 19 of the configuration, port-security A12 learn-mode static address-limit 5 mac-address 00306EA7D2E8 00306EA7D200, will yield an error similar to the following.

```
line: 19. Mac-Address is already configured in Vlan-L3-Mac.
Corrupted download file.
```

- **Config (PR_0000014818)** — Although the switch CLI provides an appropriate error message when the user tries to add more MAC addresses than a port is configured to allow, it seems to save the excess MAC addresses and display them in the configuration.

Release K.13.53

The following problems were resolved in release K.13.53. (Never released.)

- **CLI (PR_0000009868)** — Execution of a **show** command in one Telnet or console session prevents successful execution of a **show** command in a concurrent management (CLI) session.
- **TELNET (PR_0000008234)** — When a user Telnets from one switch's CLI to a second switch's CLI, and then logs out from the session on the second switch, the CLI message, "telnet connection reset by peer," is inappropriately displayed.
- **Syslog (PR_0000008241)** — Event log messages with a severity of "E" (error) are not always supported by default on syslog servers. This fix updates the show logging help text to clarify the dependency. In order to modify the syslog configuration file on a Linux server in order to receive error messages, complete the following steps.

```
1)    # vim /etc/syslog.conf                                          2)    Add
the following line in the syslog.conf file:
*.*     /var/log/messages                                          3)
# /etc/init.d/syslog   restart
```

- **Syslog (PR_0000012167)** — Syslog messages longer than 119 characters get truncated.
- **Console (PR_0000008235)** — The CLI command **console local-terminal** should affect only the session in which the command is issued, but instead it is persistent for any subsequent connections that use the same session number.
- **Crash (PR_0000010915)** — Deletion of a VLAN or creation of a trunk group from the CLI during a Telnet session from another switch may cause an unexpected reboot with a message similar to one of the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:                        Stack
Frame=0x088bf120 HW Addr=0xc3d2e1f0 IP=0x008631c0 Task='mSnmpCtrl' Task ID =0x88bf6a0
fp: 0xc3d2e1f0


Software exception at iputil_integrity.c:3054                                -
- in 'mIpCtrl', task ID = 0x1a4a0640
```

Release K.13.54

The following problems were resolved in release K.13.54. (Never released.)

- **Transceiver Configuration (PR_0000016357)** — Software version K.13.52 does not allow the HP ProCurve Gigabit 1000T MiniGBIC (J8177B/C) to be configured for several features.

Release K.13.55

The following problems were resolved in release K.13.55. (Not a public release.)

- **Config (PR_0000016767)** — There may be configuration compatibility problems with reference to the 1000T-SFP transceiver on software version K.13.54.

Release K.13.56

The following problems were resolved in release K.13.56. (Never released.)

- **Boot ROM (PR_0000015884)** — The K.12.17 ROM version is introduced to address slow switch initialization.
- **VRRP (PR_0000016192)** — In a VRRP topology with only VRRP Backups configured (i.e. there is no Master/Owner present in the setup), initializing the VRID(s) on both Backups at exactly the same time (e.g. after loss and restoration of power to all switches at once) can lead to a situation where both Backups will enter a continuous sequence of failovers.
- **Crash Messaging (PR_0000015799)** — Important data may be truncated from the crash message.
- **Crash (PR_0000015804)** — When there is a heavy volume of routing table changes, the switch may unexpectedly reboot and report a message similar to the following.

```
SubSystem 0 went down:
Software exception at alloc_free.c:435 -- in 'mIpPktRecv',
task ID = 0x85624f0 -> No msg buffer
```

- **Crash (PR_0000016373)** — Switches with heavy routing and ARP activity may experience an unexpected reboot and report the following event log message and one of the following or a similar crash messages.

  Event Log:

  W 02/08/08 17:23:18 00436 NETINET: 1 route entry creation(s) failed.

  Crash Messages Possible:

  PPC Data Storage (Bus Error) exception vector 0x300:
  Stack Frame=0x08564480 HW Addr=0x4b5a6978 IP=0x0095ce28 Task='mIpPktRecv'
  Task ID=0x8564940 fp: 0xc0206921 sp:0x08564540 lr:0x0095cd90

  PPC Data Storage (Bus Error) exception vector 0x300:
  Stack Frame=0x080b4da8 HW Addr=0x2f830000 IP=0x00867238 Task='mLinkTest'
  Task I0 fp: 0x0925aef0

  PPC Data Storage (Bus Error) exception vector 0x300:
  Stack Frame=0x088b2b88 HW Addr=0x4b5a6978 IP=0x0095c170 Task='mSnmpCtrl'
  Task ID=0x88b3190 fp: 0xc0206921

  PPC Program exception vector 0x700:
  Stack Frame=0x088b2960 HW Addr=0x0badbad0 IP=0x00000080 Task='mSnmpCtrl'
  Task ID =0x88b3190 fp: 0x008ecf3c sp:0x088b2a20 lr:

PPC Program exception vector 0x700:
Stack Frame=0x0856af90 HW Addr=0x0badbad0 IP=0x09529d14 Task='mIpCtrl'
Task ID=0 fp: 0x00000001 sp:0x0856b050 lr:0x

SubSystem 0 went down: 02/08/08 22:11:41
Software exception at alloc_free.c:435 -- in 'mIpPktRecv',
Task ID = 0x8564910 -> No msg buffer

- **Crash (PR_0000015286)** — A switch configured for routing and PIM-SM may reboot unexpectedly due to depletion of the message buffer. The switch would then report a message similar to the following.

  Software exception at alloc_free.c:439 -- in 'mIpCtrl',
  Task ID = 0xa96da80 -> No msg buffer

- **IGMP (PR_0000009415)** — The switch may intermittently fail to forward a multicast stream.
- **IGMP (PR_0000014293)** — When forced fast leave (FFL) is in use, a GMP leave sometimes terminates the stream before the appropriate timeout. Additionally, the FFL timeout value configured is not honored.
- **Logging (PR_0000003908)** — PIM errors may be inadequate for problem isolation and troubleshooting. This fix enhances the PIM error messages with more descriptive information.
- **PIM-SM (PR_0000011001)** — A Designated Router (DR) is a router directly connected to a multicast source in a PIM-SM domain. The DR notifies the Rendezvous Point (RP) of the attached multicast sources. In some cases, the DR does not notify the RP of a source, causing the multicast stream to become unavailable.
- **PIM-SM (PR_0000011070)** — The Designated Router (DR) may not transition appropriately from a Rendezvous Point Tree (RPT) or shared tree to a Shortest Path Tree (SPT), even when the source-specific SPT had the preferred route in the unicast routing table.
- **PIM-SM (PR_0000010035)** — When a routing update is given to PIM as part of a group of several updates, only the first route is updated and the switch does not properly handle subsequent unicast routing changes.
- **PIM-SM (PR_0000011801)** — PIM-SM fails to appropriately switch back to the Rendezvous Point Tree when there is a device failure on the Shortest Path Tree.
- **PIM-SM (PR_0000004569)** — Configuration of **ip pim-sparse hello-interval** does not take affect until the switch is rebooted.
- **PIM-SM (PR_0000013537)** — PIM-SM is not correctly forwarding some fragmented tunneled packets, which is causing multicast traffic to be dropped.
- **PIM-SM (PR_0000006729)** — One or more of the following symptoms may occur.
  - There may be multicast stream failure from the Designated Router to the Rendezvous Point router.
  - A failure to move appropriately from Rendezvous Point Tree to Shortest Path Tree occurs, so that a less optimal route through the network is used.
  - A prune, immediately followed by a join, could be inappropriately sent.
  - The routing switch is not processing the last entry of a compound join.
  - Prunes or joins may intermittently be sent on the wrong interface.
  - In a many-to-many multicast topology, there may be stream failure on devices residing between the DR and the RP routers.
  - Joins may be incorrectly sent when all of the joins should have aged out.
  - Some receivers are not receiving a flow until the mroute table times out.
- **PIM-SM (PR_0000011057)** — Per RFC4601, the Designated Router is supposed to send another Register message prior to expiration of the Register-Stop-Timer. This fix corrects the Register-Stop-Timer.

Release K.13.57

The following problems were resolved in release K.13.57. (Never released.)

- **Port Communication (PR_0000004568)** — An Intel NIC using the 82566DM chipset may send fragments to the switch which results in the loss of communication on that or another port, regardless of a continuous connection. Symptoms may include one or more of the following behaviors.
  - Rx Bytes counter does not increment
  - CRC/alignment errors
  - Duplex mismatch
  - Collisions, runts
  - Giants
  - Other physical layer errors

  Symptoms improve or resolve with updated NIC firmware and/or drivers, when they are available from the device manufacturer.

Release K.13.58

The following problems were resolved in release K.13.58.

- **Crash (PR_0000018180)** — The switch may reboot unexpectedly during PIM-SM configuration and display a message similar to the following.

  ```
  Software exception at pim_sm_ctrl.c:376 -- in 'mPimsmCtrl'
  ```

Release K.14.03

The following enhancements, present in K.13.40 and newer K.13 versions, are NOT present in K.14.03:

Enhancement (PR_0000003127) — Link Trap and LACP Global Enable/Disable.

Enhancement (PR_0000003128) — The ability to clear statistics was added.

Enhancement (PR_0000003718) — The MAC Lockout limit was increased to 64.

Enhancement (PR_0000007388) — The ability to configure logging via SNMP was added.

The following enhancement, present in K.13.43 and newer K.13 versions, is NOT present in K.14.03:

Enhancement (PR_0000003557) — The ability to enable/disable the USB port via CLI and SNMP was added.

The following enhancements, present in K.13.51 and newer K.13 versions, are NOT present in K.14.03.

Enhancement (PR_0000003144) — Support was added for multiple RADIUS groups.

Enhancement (PR_0000003141) — Support was added for SSH Secure to RADIUS authentication.

Enhancement (PR_0000000083) — Support was added for a MAC-Auth failure HTTP Redirect option.

The following enhancements, present in K.13.52 and newer K.13 versions, are NOT present in K.14.03.

Enhancement (PR_0000013786) — Support was added for source IP identification.

Enhancement (PR_0000008243) — Support was added for an eavesdrop prevention option.

The following problems were resolved in release K.14.03.

- **Self Test (PR_0000009650)** — In some cases, when a bank of ports fails on the yl switches, the failure status is not appropriately recognized and reported in the switch's event log.
- **CLI (PR_0000009868)** — Execution of a **show** command in one Telnet or console session prevents successful execution of a **show** command in a concurrent management (CLI) session.
- **TELNET (PR_0000008234)** — When a user Telnets from one switch's CLI to a second switch's CLI, and then logs out from the session on the second switch, the CLI message, "telnet connection reset by peer," is inappropriately displayed.
- **Console (PR_0000008235)** — The CLI command **console local-terminal** should affect only the session in which the command is issued, but instead it is persistent for any subsequent connections that use the same session number.
- **Crash (PR_0000010915)** — Deletion of a VLAN or creation of a trunk group from the CLI during a Telnet session from another switch may cause an unexpected reboot with a message similar to one of the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:
Stack Frame=0x088bf120 HW Addr=0xc3d2e1f0 IP=0x008631c0
Task='mSnmpCtrl' Task ID =0x88bf6a0 fp: 0xc3d2e1f0
```

```
Software exception at iputil_integrity.c:3054
-- in 'mIpCtrl', task ID = 0x1a4a0640
```

- **Crash Messaging (PR_0000015799)** — Important data may be truncated from the crash message.
- **Crash (PR_0000015286)** — A switch configured for routing and PIM-SM may reboot unexpectedly due to depletion of the message buffer. The switch would then report a message similar to the following.

```
Software exception at alloc_free.c:439 -- in 'mIpCtrl', task ID = 0xa96da80 -> No msg
buffer
```

- **IGMP (PR_0000014293)** — When forced fast leave (FFL) is in use, a GMP leave sometimes terminates the stream before the appropriate timeout. Additionally, the FFL timeout value configured is not honored.
- **Logging (PR_0000003908)** — PIM errors may be inadequate for problem isolation and troubleshooting. This fix enhances the PIM error messages with more descriptive information.
- **PIM-SM (PR_0000011001)** — A Designated Router (DR) is a router directly connected to a multicast source in a PIM-SM domain. The DR notifies the Rendezvous Point (RP) of the attached multicast sources. In some cases, the DR does not notify the RP of a source, causing the multicast stream to become unavailable.
- **PIM-SM (PR_0000011070)** — The Designated Router (DR) may not transition appropriately from a Rendezvous Point Tree (RPT) or shared tree to a Shortest Path Tree (SPT), even when the source-specific SPT had the preferred route in the unicast routing table.
- **PIM-SM (PR_0000010035)** — When a routing update is given to PIM as part of a group of several updates, only the first route is updated and the switch does not properly handle subsequent unicast routing changes.
- **PIM-SM (PR_0000011801)** — PIM-SM fails to appropriately switch back to the Rendezvous Point Tree when there is a device failure on the Shortest Path Tree.
- **PIM-SM (PR_0000004569)** — Configuration of **ip pim-sparse hello-interval** does not take affect until the switch is rebooted.
- **PIM-SM (PR_0000013537)** — PIM-SM is not correctly forwarding some fragmented tunneled packets, which is causing multicast traffic to be dropped.

- **PIM-SM (PR_0000006729)** — One or more of the following symptoms may occur.
  - There may be multicast stream failure from the Designated Router to the Rendezvous Point router.
  - A failure to move appropriately from Rendezvous Point Tree to Shortest Path Tree occurs, so that a less optimal route through the network is used.
  - A prune, immediately followed by a join, could be inappropriately sent.
  - The routing switch is not processing the last entry of a compound join.
  - Prunes or joins may intermittently be sent on the wrong interface.
  - In a many-to-many multicast topology, there may be stream failure on devices residing between the DR and the RP routers.
  - Joins may be incorrectly sent when all of the joins should have aged out.
  - Some receivers are not receiving a flow until the mroute table times out.
- **PIM-SM (PR_0000011057)** — Per RFC4601, the Designated Router is supposed to send another Register message prior to expiration of the Register-Stop-Timer. This fix corrects the Register-Stop-Timer.

Release K.14.04 through K.14.08

Software never built.

Release K.14.09

The following problems were resolved in release K.14.09.

- **Enhancement (0000017065)** — Support was added for the HP ProCurve 6600 Switch Premium License (J9305A) features.
- **Crash (PR_ 0000017075)** — The switch may reboot unexpectedly after GVRP is disabled from a switch, displaying a message similar to the following.

  ```
  Restricted Memory Exception number: 0xdead0100 HW Addr=0xe59ff094 IP=0x10569748
  Task='mGvrpCtrl'
  ```

- **IGMP (PR_0000009415)** — The switch may intermittently fail to forward a multicast stream.
- **Port Communication (PR_0000004568)** — An Intel NIC using the 82566DM chipset may send fragments to the switch which results in the loss of communication on that or another port, regardless of a continuous connection. Symptoms may include one or more of the following behaviors.
  - Rx Bytes counter does not increment
  - CRC/alignment errors
  - Duplex mismatch
  - Collisions, runts
  - Giants
  - Other physical layer errors

  Symptoms improve or resolve with updated NIC firmware/drivers, when they are available from the device manufacturer.
- **Flow Control (PR_0000015824)** — Fiber links may not communicate changes in flow control status appropriately to the link partner.
- **Bandwidth Limiting (PR_0000016255)** — The switch will not access a valid value of 0 (zero) for the maximum ingress bandwidth on a port.

- **Configuration (PR_0000017015)** — Configurations which utilize multiple switch features pushed to their maximum values may take an extended period to load, or cause an unexpected reboot with a message similar to the following.

```
NMI event HW:PC=0x10e8350c sp:0x12a8844c Suspects: eRouteCtrl[92]
InetServer[6]
```

- **IPv6 (PR_0000017078)** — A valid IPv4 loopback address is required, at a minimum, for IPv6 addresses to be configured. This fix notifies the user of this caveat during configuration.
- **Crash (PR_0000017354)** — Disabling debug which had been previously logging to the switch buffer may cause the switch to reboot unexpectedly with a message similar to the following.

```
Software exception at exception.c:621 -- in 'mDebugCtrl',
Task ID = 0x89ff620 -> Memory system error at 0x7c58450 - memPartFree
```

- **CLI (PR_0000014002)** — There are multiple problems with output from the CLI command show ipv6 routers which make the output either inaccurate or confusing.
- **Meshing (PR_0000017406)** — A switch participating in meshing may run out of packet buffer space and stop communicating with the other switches in the network.
- **Spanning Tree (PR_0000017820)** — Path costs are not appropriately updated after addition or removal of distributed trunks from the configuration.

Release K.14.10

The following problems were resolved in release K.14.10. (Never released.)

- **Enhancement (PR_0000011224)** — Support was added for chassis locator LED status with the CLI. For more information, see “Release K.14.10 Enhancements” on page 62.
- **Enhancement (PR_0000011601)** — Support was added for an increased number of LACP trunk groups. For more information, see “Release K.14.10 Enhancements” on page 62.
- **Enhancement (PR_0000010201)** — Support was added for SNTP client authentication. For more information, see “Release K.14.10 Enhancements” on page 62.
- **Enhancement (PR_0000013247)** — Support was added for the **show VLANs custom** CLI commands.For more information, see “Release K.14.10 Enhancements” on page 62.

Release K.14.11 through K.14.13

Versions K.14.11 through K.14.13 were never built.

Release K.14.14

The following problems were resolved in release K.14.14. (Never released.)

- **Crash (PR_0000015746)** — A very busy switch with a large configuration may experience multiple module resets, displaying event log messages similar to the following.

```
chassis: Slot A: Lost Communications detected - Heart Beat Lost(51)
chassis: Slot J: Msg loss detected - no ack for seq # 15803
chassis: Slot G: Msg loss detected - no ack for seq # 16654
chassis: Slot F: Msg loss detected - no ack for seq # 17472
```

```
chassis: Slot C: Msg loss detected - no ack for seq # 19015
chassis: Slot J: Lost Communications detected - Source Message System(48)
chassis: Slot G: Lost Communications detected - Source Message System(50)
chassis: Slot F: Lost Communications detected - Source Message System(55)
chassis: Slot C: Lost Communications detected - Source Message System(4B)
```

- **Loop Protection (PR_0000037759)** — Loop-protect may detect a loop and report that the port is shut down when it is not. This allows the loop-protect packets to flood the network and potentially starve spanning-tree and other protocols.

Release K.14.15

The following problems were resolved in release K.14.15.

- **10-GbE (PR_ 0000038110/0000038298)** — 10-GbE SFP+ transceivers may fail to form a stable link, and 10-GbE X2 transceivers may fail to initialize entirely or initialize only after a long delay.

Release K.14.16 through K.14.19

Software never built.

Release K.14.20 through K.14.23

Software never released.

Release K.14.24

The following problems were resolved in release K.14.24.

- **OSPF ECMP (PR_0000039060)** — ECMP does not route correctly to a /32 route when there are two or more paths to the destination.
- **Crash (PR_0000017435)** — Configuring a switch using the CLI command **include-credentials** may cause an unexpected reboot if the switch has never had the feature previously enabled. The crash message may vary.
- **Loop Protection (PR_0000037759)** — Loop-protect may detect a loop and report that the port is shut down when it is not. This allows the loop-protect packets to flood the network and potentially starve spanning-tree and other protocols.
- **Crash (PR_0000038523)** — Hot-swapping transceivers too quickly may cause the switch to reboot unexpectedly with a software exception. Best practice tip: Each time a transceiver is inserted into the switch, allow it to fully initialize prior to removing it. The crash message may be similar to the following, though it may vary.

  ```
  Software exception in ISR at svc_timers.c:472
  ```

- **Crash (PR_0000037527)** — The switch may reboot unexpectedly when loading an extensive configuration. The crash message may be similar to the following.

  ```
  No msg bufferon at alloc_free.c:439 -- in 'mIpCtrl',
  task ID = 0xa96bb80
  ```

- **10-GbE (PR_0000038110)** — 10-GbE SFP+ transceivers may fail to form a stable link.

- **CLI Wizard (PR_0000038179)** - The Management Interface Setup Wizard (invoked using the CLI command setup mgmt-interfaces) provides a generic error message of *inconsistent value* when an attempt is made to save a configuration with an invalid value.
- **SNMP (PR_0000038253)** — There are duplicate entries in the hpicfTC.mib for the 10-GbE SFP+ Direct Attach Cables.
- **10-GbE SFP+ DAC Transceiver (PR_0000038570)** — When a port that contains an SFP+ Direct Attach Cable on an HP ProCurve 6600 Series Switch is disabled, the switch stops sending traffic to the port but the transceiver on the other end of the cable is not aware of the link loss. This could be particularly problematic if the port is part of a static HP Trunk.
- **SNMP (PR_0000039064)** — The SNMP index for the ports on the 6600-48G switches, referenced in the **hpicfOid.mib**, is not correct.
- **SNTP Authentication (PR_0000037553)** — The switch CLI does not allow configuration of the maximum key-value string of 32 characters for SNTP Authentication.
- **Crash (PR_0000038615)** — The switch may reboot unexpectedly with a message similar to the following.

```
Software exception at ipamSApi.c:66 -- in 'mIpAdMUpCt'
```

Release K.14.25

Software never built.

Release K.14.26

The following problems were resolved in release K.14.26.

LLDP (PR_0000038230) — The length of a CDP packet may prevent the switch from accepting the packet.

Proxy-ARP (PR_0000038934/0000038938) — The switch may provide proxy-ARP replies to gratuitous-ARPs, which could be interpreted as a "duplicate IP address" by the original sending host.

Proxy-ARP (PR_0000038935) — The switch may provide proxy-ARP replies to ARPs from a source IP address that is not within the scope of the switch's IP address/subnet mask.

DHCP-Snooping (PR_0000019155) — DHCP-Snooping does not correctly identify fragmented packets, and drops UDP Fragments if a hex value of 44 (68 decimal) is present in the payload where the header is usually located (in a non-fragment).

Release K.14.27 through K.14.29

Software never built.

Release K.14.30

Software never released.

Release K.14.31

The following problems were resolved in release K.14.31.

- **Flow Control (PR_0000038853)** — When flow control is enabled on the switch, execution of the **show int brief** CLI command reveals that flow control is not actually enabled on gigabit or dual-personality ports.
- **Flow Control (PR_0000038851)** — When flow control is disabled on one or more interfaces via the CLI, execution of the **show int brief** CLI command reveals that the change in flow control status does not take effect unless the switch is reloaded.
- **OSPF (PR_0000038751)** — A switch configured for OSPF on both a VLAN and a loopback interface will report the following in the event/debug log, due to improper treatment of the loopback address.

  ```
  OSPF: invalid packet: Packet with same router id as ours (28)
  ```

- **Crash (PR_0000039470)** — A very busy switch configured with jumbo frames, OSPF routing, DHCP-snooping, QoS priority assignment, and Web-based authentication may reboot unexpectedly with a software exception. The crash message may vary.
- **Virus Throttling/IGMP (PR_0000040124)** — When a switch is configured for IP IGMP and Virus Throttling (connection-rate filtering), if the rate of joins sent by a host triggers a "block" by the Virus Throttling, the following software exceptions are seen in the switch event log. No other symptoms have been observed except the lines in the log. Multicast traffic still goes through. The port is not blocked as expected.

  ```
  00805 connfilt: Unable to block 124.2.0.211 in hardware, <port>

  sys: 'Software exception at vt.c:1065 -- in 'mIpPktRecv', task ID = 0xa977e40'

  sys: 'Software exception at aqTcamInterface.c:829 -- in 'mIpPktRecv', task ID =
  0xa977e40'

  00805 connfilt: Unable to block 124.2.0.210 in hardware, <port>

  sys: 'Software exception at vt.c:1065 -- in 'mIpPktRecv', task ID = 0xa977e40'

  sys: 'Software exception at aqTcamInterface.c:829 -- in 'mIpPktRecv', task ID =
  0xa977e40'

  00805 connfilt: Unable to block 124.2.0.212 in hardware, <port>

  sys: 'Software exception at vt.c:1065 -- in 'mIpPktRecv', task ID = 0xa977e40'

  sys: 'Software exception at aqTcamInterface.c:829 -- in 'mIpPktRecv', task ID =
  0xa977e40'
  ```

Release K.14.32

The following problems were resolved in release K.14.32.

- **Port Communication (PR_0000018161)** — On some driver/firmware revisions, the Intel 82566DM and 82566DM-2 gigabit NIC chipsets may send an excessive number of corrupt packets. This traffic may affect communication on the port attached to the problem NIC, or on another port on the same module or port-bank. This fix helps to ensure continued communication by downgrading the port setting to auto-10/100, and logging an FFI message in the event log. The event log message will be similar to the following, and will indicate the port that is receiving the problem traffic. Please check with your PC vendor to see if there is an updated firmware version available for the affected NIC.

  ```
  02671 FFI: Port <number> has been downgraded to 10/100.
  See www.procurve.com/device_help/nic_update for details.
  ```

- **Authentication (PR_0000011138)** — If the Radius server becomes unavailable, the **eap-radius authorized** option allows the switch to authenticate devices. If the response time of the RADIUS subsystem is greater than the server-timeout value on the switch or the device supplicant then the switch will not be able to authenticate devices, and no warning of this failure will be displayed. This fix triggers the display of the following CLI message.

  ```
  The RADIUS connection timeout must be less than the authentication server timeout for
  the switch to authenticate automatically when the RADIUS server is unavailable.
  ```

- **ACL/QoS (PR_0000017975)** — When an ACL permit statement specifies a TCP or UDP port number or range, non-initial fragments of these TCP or UDP packets may not be acted upon in the same manner as the initial fragment, potentially causing some inappropriate drops.

- **Port Communication (PR_0000017032/0000037992)** — Invalid/corrupt packets sent to the switch by a NIC operating at gigabit speed may trigger a loss of communication on a different port that shares the same ASIC. In that case, the port will retain its link and the Rx bytes, ifInDiscards, and the Discard Rx counters increment. Prior to this fix, communication on the port could only be reliably recovered by switch reload. This problem may also be associated with the following event log messages.

  ```
  00374 chassis: Slot <x> Slave ROM Tombstone: 0x13000601
  00374 chassis: Slot <x>: Lost Communications detected - Heart Beat Lost
  ```

- **FFI/Config (PR_0000039989)**
  - **FFI** - If an FFI event is triggered, and then the link is brought down and back up again, the same FFI event will be triggered again in about 20 seconds even if the trigger condition isn't met.
  - **Config** - Configuration changes made for PR_0000018161 (see page 214) are not visible to the user; it appears that a port configured at both the NIC and the switch for auto-gig is operating at 100FDx for no reason (particularly if the associated event log message has scrolled out of the switch log). This fix makes the downgrade of the port to auto-10/100 visible in the running configuration. Note that this may trigger the switch to ask "Do you want to save current configuration?" upon logout or switch reload.

- **RADIUS Accounting (PR_0000012487)** — The switch doesn't send an accounting-stop when a switch **reload** closes the session.

- **CLI (PR_0000018670)** — Execution of the CLI command **show tech all** on a switch may trigger the switch to become unresponsive and require a power-cycle to recover.

- **CLI (PR_0000018594)** — Attempts to utilize the CLI interface configuration command **mdix-mode mdix** yields an error setting value mdix for port <port number>.

- **Authentication (PR_0000016211)** — If no RADIUS server is accessible during a re-authentication attempt, the clients will remain connected to an auth-vid even if an unauth-vid was defined.

- **10-GbE SFP+ DAC Transceiver (PR_0000039363)** — The "A" version of the J9281A HP ProCurve 10-GbE SFP+ 1m Cable, J9283A HP ProCurve 10-GbE SFP+ 3m Cable, and J9285A HP ProCurve 10-GbE SFP+ 7m Cable does not comply with the January 2009 version of the Multi-Source Agreement (MSA), SFF-8472 Rev 10.4. The result is interoperability problems that may prevent a link from becoming established. This fix adds support for the "B" version Direct Attach Cables (DACs): J9281B, J9283B, and J9285B. The "B" version DACs are compliant with MSA SFF-8472 Rev 10.4. Additionally, the "B" version DACs interoperate with the Intel NIC (Intel 10 Gigabit AF DA Dual Port Server Adapter).

- **Switch Hang (PR_0000014307)** — A switch with 802.1X configured may stop passing AAA requests and routed traffic. Over time this issue manifests itself in the form of lost TELNET and SSH access, and eventually even console access to its management is lost. Clients that attempt to authenticate will get a "domain not available" message. The switch must be reloaded to recover from this state.

- **VRRP (PR_0000016626)** — VRRP may show failovers or near failovers without any apparent reason.

- **Port Communication (PR_0000039476)** — Ports on zl switches configured for 10/100 may get into a state where connectivity is compromised. The network icon in the PC system tray shows limited or no connectivity. The PC does not get a DHCP address, and the switch Rx counters do not increment. If the PC is moved to another port the client PC comes up. The switch port is recoverable by configuring it down to 10-Mb operation, then back to 10/100.
- **Appletalk ARP (PR_0000015652)** — Appletalk ARP (AARP) packets are not traversing the Protocol VLAN, which makes file sharing and print services unavailable.
- **802.1X (PR_0000010850)** — If an unauth-vid is configured, and the client limit is reached on a switch port, a properly credentialed re-authentication following an improperly credentialed authentication attempt (for example, incorrect password) will leave the 802.1x client in the unauthorized VLAN instead of applying the appropriate authorized VLAN.
- **Web/FFI (PR_0000040095)** — The Web Management Interface Alert Log message does not match the FFI log message for PR_0000018161 on page 214.

Release K.14.33

The following problems were resolved in release K.14.33.

- **Web Authentication (PR_0000041695)** — Web authentication for port-access does not function on software version K.14.32.
- **CLI (PR_ 0000038243)** — When task-monitor is enabled, the CLI output from the command **show cpu** is inconsistent with the sub-task averages, and higher than it should be. This behavior does not change after disabling task-monitor.

Release K.14.34

The following problems were resolved in release K.14.34.

- **Enhancement (PR_0000042932)** — Support is added for the following new products.
  - J9475A - HP ProCurve 8206zl Switch Base System
  - J9307A - HP ProCurve 24-Port 10/100/1000 PoE+ zl Module
  - J9308A - HP ProCurve 20-Port 10/100/1000 PoE+/4-port MiniGBIC zl Module
  - J9478A - HP ProCurve 24-port 10/100 PoE+ zl Module
  - J9447A - HP ProCurve 5406zl-48G-PoE+ Switch
  - J9448A - HP ProCurve 5412zl-96G-PoE+ Switch
- **Jumbo Frames (PR_0000042090)** — When a non-default jumbo frame size is present in the configuration (e.g. if the following lines are present in the config **jumbo max-frame-size 9000** and **jumbo ip-mtu 8982**), sometimes the default jumbo frame size is used by the switch, rather than the configured parameter.
- **Crash (PR_0000040685)** — A highly stressed switch may reboot unexpectedly with a message similar to the following.

  ```
  Software exception at svc_misc.c:668 -- in 'mSnmpCtrl',
  task ID = 0xa941a40     -> No memory available
  ```

- **Crash (PR_0000040369)** — When a highly stressed switch has the power save feature enabled (using the CLI command **savepower module all**) and disabled (using the CLI command **no savepower module all**) repeatedly, it may reboot with a software exception, logging a crash message similar to the following.

  ```
  Software exception at buffers.c:2380 -- in 'mFtrEvtMgr', task ID = 0xa935f00
  ```

- **Crash (PR_0000039922/ 0000040170)** — The switch may reboot unexpectedly or become unresponsive when the CLI command **erase startup-config** is executed. There may be a message similar to the following after the event.

  ```
  Software exception in kernel context at ghsException.c:1037
  -> Internal system error
  ```

- **PoE (PR_0000039837)** — When the internal switch power is turned off (or fails) while an external power supply is connected, PoE becomes disabled and will not re-enable. The following event is logged in the switch.

  ```
  W <date> <time> 00274 chassis: (81): Co-Processor Crash detected - Available 0
  ```

- **Jumbo Frames (PR_0000039218/0000039705)** — Jumbo frame configuration does not behave appropriately following module hotswap, resulting in jumbo frames either being forwarded when they exceed the maximum **ip-mtu** value.
- **CLI (PR_0000039292)** — Output from the CLI command **show modules** shows modules as "Failed" during self test; this fix changes the display to read "Booting".
- **Transceivers (PR_0000039218)** — When an unsupported transceiver is present during initial power-up, the LED should blink amber, but does not. Additionally, the slot then fails to detect removal of the transceiver.
- **Module Crash (PR_00000038682)** — When a 12-slot zl chassis is running on less than the supported minimum of 2 power supplies, sometimes all 12 modules fail. What should happen is that the upper 6 slots remain powered and the lower 6 slots fail to be powered. Note: When the minimum of 2 power supplies is restored, the lower 6 modules, if present, need to be re-inserted or the chassis rebooted in order to restore power to those slots.
- **CLI (PR_00000038356)** — When a module is removed and another type is inserted, the information from the initial module (including the serial number) may still be present in response to the CLI command **show modules**.
- **Temperature (PR_0000017072)** — The 8200zl switch chassis temperature threshold is incorrectly set to 55 degrees C, rather than the 40 degrees C it should be.
- **Temperature (PR_0000015290)** — The 6200yl and 3500yl switch temperatures are incorrectly elevated between 6-8 degrees C as observed in the switch response to the CLI command **show system temperature**. As a result, over-temperature messages are being incorrectly triggered. Event log messages will look like the following.

  ```
  <date> <time> 00553 chassis: Over Temperature: Chassis Intake Air
  ```

- **Temperature (PR_0000010540)** — The 6200yl and 3500yl switch temperature thresholds are incorrectly set to 40 degrees C, even when there are no 10-GbE transceivers installed in the HP ProCurve Switch yl 10-GbE 2-Port CX4 + 2-Port X2 Module (J8694A).

Release K.14.35

The following problems were resolved in release K.14.35

- **Enhancement (PR_0000042908)** — Support is added for the following new products.
  - J9443A - HP ProCurve 630 Redundant/External Power Supply
  - J9309A - HP ProCurve 4-Port 10Gbe SFP+ zl Module

Release K.14.36

Software never built.

Release K.14.37

The following problems were resolved in release K.14.37. (Not a public release)

- **Enhancement (PR_0000040368)** — Support is added for the following new products.
  - J9300A - HP ProCurve 10-GbE XFP-SFP+ 1m Direct Attach Cable
  - J9301A - HP ProCurve 10-GbE XFP-SFP+ 3m Direct Attach Cable
  - J9302A - HP ProCurve 10-GbE XFP-SFP+ 5m Direct Attach Cable
- **Web Authentication (PR_0000041695)** — Web authentication for port-access does not function.
- **CLI (PR_0000000912)** — The CLI command **copy tftp show-tech** fails, resulting in failure to create a custom show-tech file on the switch.
- **Config (PR_0000041803)** — The config lines for **aaa authentication** and **aaa accounting** appear in the wrong order in the running-config; these configuration parameters are dependent upon the **radius-server** and **aaa server-group**, and therefore need to follow those settings in the configuration.
- **SNMP (PR_0000014902)** — SNMP traps contain the wrong instance number for the event Description (the **eventDescription** is one instance number too low).
- **CLI (PR_0000013912)** — The HP ProCurve Redundant Wireless Services **zl** Module (J9052) is incorrectly reported by the switch CLI as an **xl** module.
- **Enhancement (PR_0000016944)** — Log OSPF Adjacency Changes. See page 81 for a detailed description.
- **Event Log (PR_0000038339)** — The switch records an event log message when a specific user's ACL/ACE cannot be added, but does not give any indication if all the switch ACE resources have been consumed.

  Original log message: `00700 idm: Unable to add ACL entry, ace index`

  `3, client mac <MAC address>, port <number>`

  New log message: `00055 ACL: unable to apply ACL <client MAC address>,`

  `failed to add entry 23, max ACE limit reached`
- **CLI (PR_0000015982)** — Using the port-security feature, attempts to enter more than the configured MAC address limit on a port result in an ambiguous error message: `Inconsistent value`. This fix triggers a more appropriate error message: `Warning: Number of configured addresses on port <port number> exceeds address-limit.`
- **Config (PR_0000018749)** — If MSTP instance port settings (port priority or path cost) are configured prior to link aggregation, once a trunk group is configured, the MSTP instance configuration lines reference the individual ports (errant behavior) and not the trunk group (expected behavior). As a consequence, the switch will not be able to reload the configuration because the MSTP instance port settings are invalid.
- **MAC Authentication (PR_0000015520)** — Traffic from unauthenticated clients may be allowed during the process of authenticating clients under heavy loads.
- **SSH (PR_0000040877)** — When an exit from a switch management SSH session is initiated from an SSH client, the termination values from the switch are incorrect, triggering the following erroneous message to be displayed at client: "`SSH connection is closed by remote host`".
- **Crash (PR_0000002449/0000002511)** — The switch may reboot unexpectedly with a software exception when MSTP and meshing are both configured.

- **Crash (PR_0000039155)** — A module may reboot and report a crash message similar to the following when IPv6 ACLs or policies are applied at either the CLI or through IDM.

  ```
  Software exception at aqTcamSlaveHwBttfClone.c:1332 -- in 'mAsicUpd', task ID = 0x61e7140
  ```

- **CLI (PR_0000016116)** — When the **include** parameter is used with a **show** command, and the switch finds a matching regular expression, the console output contains all-zeros byte.
- **Routing (PR_0000040696)** — CPU-generated packets may have the wrong next-hop MAC address; they are sent out of the appropriate IP interface and VLAN but this may cause SNTP, ping, and other host applications to fail.
- **Crash (PR_0000038937)** — Configuring an IPV6 address followed by a routed ACL with a UDP port range applied to a VLAN may cause the modules to reset.

Release K.14.38

The following problems were resolved in release K.14.38. (Not a public release)

- **CLI (PR_0000042136)** — Output from various commands (or SNMP queries) of CPU utilization is not consistent. While the values reported by the CLI command **show cpu** is correct; **show sys** does not yield an accurate value. In addition, SNMP query of the CPU utilization, Menu navigation to CPU utilization, and Web Management Interface report of the CPU utilization is inaccurate.
- **Management (PR_0000016016)** — SSH and ping times to the switch are significantly slower on K.14 than they were on K.13 software versions.
- **BootROM (PR_0000042960)** — The boot ROM on an HP ProCurve 6600-24XG Switch does not update when the system software is updated. Note that there is no functional consequence of this failure.
- **BootROM (PR_0000042932a)** —The boot ROM required for the new products introduced in K.14.34 and K.14.35 is K.12.20; this boot ROM version will now be updated on other products sharing the software branch.
- **Crash (PR_0000016958)** - The switch may reboot unexpectedly when a second SSH session is established with the switch management while the switch is transferring a show tech custom file to a TFTP server. The crash message will be similar to the following.

  ```
  Software exception at exception.c:501 -- in 'mSess3', task ID =
  ```

  ```
  0x8280a60 -> Memory system error at 0x60 - memPartFree
  ```

- **Crash (PR_0000041168)** — Running or copying the output from the CLI command **`show tech`** causes a memory leak that will eventually result in memory depletion and switch reboot. The crash messages vary widely, and may include PPC errors, NMI errors, and "Out of resources: no token found" errors.
- **Crash (PR_0000042176/0000041586)** — Entry or upload of multi-line CLI config commands may cause the switch to reboot unexpectedly with a message similar to the following.

  ```
  PPC Data Storage (Bus Error) exception 0x300: esf=0x082e6058
  ```

  ```
  addr=0x942201fc ip=0x001c7910 Task='mSess1' tid=0x82e6b20
  ```

- **Config (PR_0000041545)** — When a switch with remote mirroring configuration is updated from K.13.xx to K.14.xx, remote mirroring destination interface is incorrectly converted.
- **10-GbE (PR_0000043292)** — Some J8438A HP ProCurve 10-GbE X2-SC ER Optics (a subset of those with serial number containing the letters DM in the middle) do not turn on the laser after the switch reboots. Workarounds: Hotswap the optic, update to a software version with the fix, or request a replacement.

- **Config (PR_0000042930)** — The (fixed) "module 1" which is usually present in the running and startup configurations is not present. Output from **show run** looks like the following.

  ```
  module 1 type
  module 2 type J86xxA
  ```

As a result, previously saved 3500yl configurations will not successfully upload to the switch. When attempts are made, it reports an error: `Invalid input: J86yyA`.

Release K.14.39

The following problems were resolved in release K.14.39. (Not a public release)

- **8200zl Management Module Compatibility (PR_0000041133)** — When exchanging a management module from an 8212zl for use as the only management module in an 8206zl chassis (or vice versa), the management module must be on a boot ROM and software version that is supported by the 8206zl, and any existing configuration on the module must be erased after the module is inserted into the target switch (using the CLI command **erase startup-config**). The switch console should prompt the administrator to perform the necessary action after module insertion, but does not.
- **Enhancement (PR_0000041910)** — The status of the 10-GBe SFP+ ports is not displayed in the Web Management Interface (Configuration > Device View) when a mouse-over of the port occurs. There should be an indication of the whether the port is enabled/disabled: the CLI accurately reflects the status, but the Web does not.

Release K.14.40

The following problems were resolved in release K.14.40. (Not a public release)

- **Enhancement (PR_0000016237)** — Port VLAN ID TLV Support on LLDP. See page 84 for detailed information.
- **Enhancement (PR_0000040732)** — Remote Mirroring Using the Loopback Interface. See page 85 for detailed information.
- **Enhancement (PR_0000038122)** — TELNET Negotiate About Window Size (NAWS) Initiation. See page 87 for detailed information.
- **Enhancement (PR_0000042815)** — When a config is uploaded to the switch containing a banner MOTD configuration that exceeds the maximum multi-line input, the following error message is now returned at the CLI: `Only 16 lines allowed in multi-line input.  Command not executed`.
- **Enhancement (PR_0000043278)** — Crash information was improved in order to speed time to resolution.
- **Enhancement (PR_0000018513)** — Banner enhancements were made. See page 88 for detailed information.
- **Enhancement (PR_0000040021)** — A Source IP Identity may now be configured for SNTP, outgoing TELNET and TFTP. See page 89 for detailed information.
- **Meshing (PR_0000044173)** — Rarely, a device may intermittently lose connectivity through the mesh.
- **Enhancement (PR_0000040721)** — Extended ping and traceroute are now available.
- **Enhancement (PR_0000040378)** — Implementation of DHCP hostname (option 12). See page 95 for detailed information.
- **Enhancement (PR_0000037664)** — DHCP-based Auto Image and Configuration Update. See page 96 for detailed information.

Release K.14.41

The following problems were resolved in release K.14.41.

- **Licensing (PR_0000043665)** — When a Services zl Module (HP ProCurve Wireless Edge Services or ONE Services zl Module) is present, and either telnet or SSH is used to communicate with the switch, the hardware ID that is reported in preparation for license registration or application activation becomes truncated. Workaround: Console to the switch to obtain a valid hardware ID.

Release K.14.42

The following problems were resolved in release K.14.42 (not a public release).

- **Crash (PR_0000041509)** — Removing a module that contains a mirror destination port may trigger one or more modules to reset.
- **Crash Messaging (PR_0000043287)** — In the case of a module heartbeat failure, crash data fails to be reported by the interface module.
- **Enhancement (PR_0000017201)** — The switch Fault Finder function has been extended to cover an improperly behaving fiber transceiver, or other condition which results in a link "flapping" rapidly between link-up and link-down states. A new fault event "link-flap" has been created to detect these events. Additionally, a new action, "warn-and-disable," has been created to report and disable the events. Together, these enhancements allow the errant condition to be detected, and the port in question optionally disabled.

Release K.14.43

Software never built.

Release K.14.44

The following problems were resolved in release K.14.44 (not a public release).

- **Redundant Management (PR_0000037617)** — Synchronization of redundant management modules on an 8200zl switch fails if there are more than 2 characters in the minor revision field of the switch system software version.
- **GVRP (PR_0000040238)** — After a dynamically-learned VLAN is converted to a static port-based VLAN, and an interface is made a static member of that VLAN, disabling GVRP causes the port to lose the VLAN membership. The running-config, startup-config and the SNMP egress static member list for the VLAN show the port as member of the VLAN. All other data shows the port is no longer a member of the VLAN. VLAN communication over the affected interface is no longer possible until the one of the two following workarounds is executed. Workarounds: Either re-issue the tag and untag commands for VLAN port assignment or reload the system.
- **QoS (PR_0000042343)** — QoS on Ports may not behave correctly when trunks are involved, e.g., if QoS is configured on a port that is a member of a trunk, the CLI command **no qos** does not disable the feature as it should.
- **ACL/QoS (PR_0000045616)** — ACL/QOS Error return definitions as measured by the hardware layer are out-of-synch with SNMP values.
- **PIM (PR_0000012391)** — When OSPF, IGMP, and PIM are all configured, the switch reaches a sustained or increasing level of > 50% CPU utilization when a multicast stream with TTL=1 is received.

- **Fault Finder (PR_0000045772)** — When the switch fault-finder feature is configured to disable a transceiver port in response to link-flapping, and the disable has occurred, fault-finder will no longer properly disable that port following transceiver hot-swap.
- **RADIUS Accounting (PR_0000042522)** — The 'class' attribute is not included in the accounting-request to the RADIUS server; RFC 2865 states that this should occur.
- **MSTP/QinQ (PR_0000041219)** — When QinQ (Provider Bridging) is operating in mixed mode, switch identification of S-VLANs (Service VLANs) and C-VLANs (Customer VLANs) may be inaccurate sometimes. As a result, the switch allows S-VLANs to be assigned as members of MSTP instances and disallows some C-VLANs from being properly assigned to an MSTP instance.
- **Management (PR_0000016049)** — If a console or telnet session to the switch is used to execute a CLI command (e.g. execution of the show tech command) and then the management session is abandoned before the task is completed (e.g. the window is closed), that session becomes unresponsive. If, at that point, another management session is established and the CLI command kill is executed to end the initial, now unresponsive session, the new management session will become unresponsive as well, until all sessions are in use and unresponsive.
- **Enhancement (PR_0000041022)** —Enhancement to AAA accounting. For more information, see “Accounting Services” on page 102.
- **UDLD (PR_0000043071)** - UDLD transmits a burst of packets when any port on the switch goes down (1 packet is sent for each port that goes down), falsely triggering a failure state.
- **Command Authorization (PR_0000043525)** — HP-Command-String authorization does not work as expected.
- **PoE (PR_0000045766)** — There are intermittent issues in the support of some pre-standard PoE phones; sometimes phones will boot and sometimes they don’t. Grouping four or more phones together in consecutive ports may trigger this issue more often.
- **GVRP (PR_0000012224)** — Changing the GVRP **unknown-vlan** state from 'block' to 'learn' and vice versa stops all GVRP advertisements from that interface until the interface is disabled and then re-enabled.
- **GVRP (PR_0000040758)** — Switches do not use multiple GARP Information Propagation (GIP) contexts when the switch has been configured for MSTP operation; the same GIP context is used for all ports participating in GVRP. There should be multiple GIP contexts - one for each 'spanning-tree' (the IST and each of the MSTIs).
- **Enhancement (PR_0000040783)** — This enhancement reduces the down time when unicast routing indicates a Candidate Rendezvous Point (C-RP) is not reachable. Upon detecting a C-RP has become unreachable, the Bootstrap Router (BSR) sends a new Bootstrap Message (BSM) with a zero holdtime for the unreachable C-RP. All devices in the PIM domain should then remove this C-RP from their RP-set.
- **Enhancement (PR_0000041395)** — Debug capability for PIM packet events is added. The command syntax is as follows.

```
ProCurveSwitch# debug ip pim packet
hello
register
join-prune
bsr
dr
rp
<cr>
```

Examples:

```
ProCurveSwitch# debug ip pim packet join
```

```
This command would show all prunes, joins, grafts, and graft-acks that are sent and received on the switch.

ProCurveSwitch# debug ip pim packet hello vlan 3,4,7-16

This command would show all hello packets sent and received on vlans 3, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16.

ProCurveSwitch# debug ip pim packet

Engages all pim packet debugging.

ProCurveSwitch# debug ip pim

Engages all pim debugging.
```

IP PIM debug output may be filtered further by specifying a source IP address, VLAN and group. Use the CLI help for syntax details.

- **PIM (PR_0000040412)** — When software is routing multicast packets, the packets are sent as CPU originated packets. As a result, features that rely on knowing the inbound source port (e.g. source port filtering) do not get applied.
- **PIM-SM (PR_0000042163)** — Multicast traffic is lost for 20-30 seconds, approximately 5 minutes after a failed-over topology has recovered.
- **PIM (PR_0000043798)** — PIM debug output has the wrong bits set for (*,G) join-prune packets.
- **PIM-SM (PR_0000045837)** — Following link failover and failback along the active data path, PIM-SM floods the UDP stream from the source to multiple RP's.
- **PIM-SM (PR_0000041446)** — When a Bootstrap Router (BSR) receives a Candidate-RP Advertisement (C-RP-Adv) with a zero holdtime, it does not send a Bootstrap Message (BSM) with a zero holdtime; instead, it stops including the C-RP in subsequent bootstrap messages.
- **Multicast (PR_0000041104)** — A software flaw was found which may have resulted in a variety of unexpected behaviors.
- **PIM-SM (PR_0000012262)** — In a topology with a statically configured rendezvous point, a client's initial join will trigger receipt of the multicast stream. However, after leaving and re-joining the group, one of the following will happen.
  - If the multicast stream address is still present in the client's local router's multicast routing table, there is a delay of up to a minute after the IGMP join before the client receives the stream
  - If the client's local router's multicast routing table has timed-out the multicast stream address, then the stream is never received by the client after it re-joins the group.
- **Crash (PR_0000040241)** — The switch may reboot unexpectedly with a message similar to the following (message may vary).

  ```
  Software exception at hwBp.c:156 -- in 'mBSRCtrl', task ID = 0x7f06db0 -> MemWatch Trigger: Offending task
  'mPimsmCtrl'. Offending IP=0x845580
  ```

- **PIM-SM (PR_0000040618)** — When the last known neighbor on an interface times out, PIM-SM fails to remove the flows which have that interface as the Reverse Path Forward (RPF) to the source. This causes the multicast streams to stop, instead of moving to the Reverse Path Tree (RPT) if possible.
- **PIM-SM (PR_0000040621)** — When information about a multicast group with any source (*,G) is received for downstream interfaces, the outbound list is only modified if it is a new *,G; it needs to be about to modify the outbound list for existing groups as well.
- **PIM (PR_0000041887)** — When a PIM router is the elected Bootstrap Router (BSR), then fails a future BSR election, it keeps stale candidate Rendezvous Point (RP) information. If this device later becomes the elected BSR again, this stale information is then included in the BSM packets created by the BSR. This can cause long delays in failovers if the stale information includes RP's which are no longer reachable.

- **PIM-SM (PR_0000042433)** — When a multicast client joins and then leaves a multicast stream, there may be a delay of approximately 20 seconds before that client can join again.
- **PIM-SM (PR_0000040622)** — When a flow is on the Reverse Path Tree (RPT) PIM-SM fails to send joins towards the source as a part of the periodic join timer. This should happen when the unicast source, multicast group (S,G) is joined and the Reverse Path Forward (RPF) for the source and Rendezvous Point (RP) differ. This causes the flow to not move to the Shortest Path Tree (SPT).
- **Crash (PR_0000041540)** — The switch may reboot unexpectedly with a message similar to the following.

  ```
  PPC DataStorage (Bus Error) in PimSmQA_TraceAndcheckSGs_SG...
  ```

- **PIM-SM (PR_0000016110)** — When the DR_Priority option is configured to a value of zero (default priority is 1), the option is no longer included in the hello message as it should be.
- **PIM (PR_0000018504)** — When a multicast stream is flowing through a PIM network using a better path (as determined by the DR) than the one through the rendezvous point, PIM does not adjust the multicast stream properly (it stops flowing) when PIM gets disabled on a VLAN along the data path.
- **PIM-SM (PR_0000042263)** — PIM may send RPT joins or prunes to itself when it is the rendezvous point.
- **PIM-SM (PR_0000042654)** — PIM may send a join or prune to a device that it inappropriately sees as an upstream neighbor.
- **PIM-SM (PR_0000043801)** — PIM is not sending compound (*,G) Prune (S,G) for SG's not joined.
- **PIM-SM (PR_0000040825)** — Candidate-Rendezvous Point Advertisement (C-RP-Adv) messages are still sent out after the Candidate RP source-VLAN is down. This results in other PIM routers in the domain continuing to send Register messages to the unavailable RP.
- **PIM-SM (PR_0000042647)** — The PIM bootstrap router (BSR) has a memory leak when static rendezvous points are used.
- **Crash (PR_0000043217)** — If a VLAN containing a candidate RP is deleted, the switch will reboot unexpectedly, recording a crash message similar to the following.

  ```
  Software exception at vls_util.c:133 -- in 'mBSRCtrl'
  ```

- **Crash (PR_0000018180)** — The switch may reboot unexpectedly during PIM-SM configuration and display a message similar to the following.

  ```
  Software exception at pim_sm_ctrl.c:376 -- in 'mPimsmCtrl'
  ```

- **RADIUS (PR_0000045092)** — The Radius A/V pair option, 'NAS-IP-Address' does not get populated when the Out of Band Management (OOBM) port is the source of the packet.

Release K.14.45

The following problems were resolved in release K.14.45 (not a public release).

- **SSH (PR_0000014531)** - Rarely, after some period of time with normal SSH connectivity, the switch may become unresponsive to further SSH management.
- **Crash (PR_0000046506)** - Execution of the CLI command **console local-terminal none** may cause the switch to reboot unexpectedly, logging a message similar to the following. Note that this problem was found and fixed on a special debug version of software; symptoms in released software, if any, may vary.

  ```
  Software exception at parser.c:2373 -- in 'mSess1', task ID = 0xa931000 -> ASSERT:  failed
  ```

Release K.14.46

The following problems were resolved in release K.14.46 (not a public release).

- **Terminal Display (PR_0000008239)** — When a switch telnet session is opened from aUnix/Linux terminal, the line wrap of the terminal is not preserved after logout.
- **CLI (PR_0000046982)** — When QinQ (Provider Bridging) is configured for mixed mode, the switch CLI does not allow port memberships to be moved from C-VLANs to S-VLANs; it returns the following error upon attempt.

  ```
  <port>: Error moving ports between c-vlans and s-vlans.
  ```

- **TFTP (PR_0000040441)** — When an attempt is made to download a configuration file from the TFTP server, there is an invalid error being logged if the config file does not exist on the TFTP server: tftp: RCVD error:0, msg:. Changes have been implemented so that the error message accurately indicates the cause of the file transfer failure.
- **Banner MOTD (PR_0000042871)** — The message returned by the CLI in response to the **banner MOTD** configuration command erroneously states that a banner of up to 3071 characters is supported; the actual maximum number of characters is 3070.
- **RADIUS (PR_0000046154)** - MAC Based Radius Sessions go unauthenticated even if cached reauth is enabled when Radius Server Groups are set
- **CLI Help (PR_0000046320)**— AAA command in-line help lists the "cached-reauth" option even after it has already been typed into that command. For example:

  ```
  ProCurve Switch 3500yl-48G(config)# aaa authentication port-access chap-radius server-group pat cached-reauth ?
  none            Do not use backup authentication methods.
  authorized      Allow access without authentication.
  cached-reauth     Grant access in case of reauthentication retaining the current session attributes.
  <cr>
  ```

The"cached-reauth" option should not be displayed, since it has already been typed in the command line.

- **Crash (PR_0000044298)** — When RADIUS accounting is enabled, entering a command with too many characters entered at the CLI will crash the switch and record an error similar to the following.

  ```
  Access Violation - Restricted Memory
  Exception number: 0xdead0000
  HW Addr=0x00000000 IP=0x00002680 Task='mftTask' Task ID=0xa941c80
  fp: 0x30442030 sp:0x042333b
  ```

- **CLI (PR_0000045556)** — Mesh ports cannot be configured to mirror or monitor. For example, when issuing the CLI command int mesh monitor, the switch reports: Unknown port type.

Release K.14.47

The following problems were resolved in release K.14.47.

- **Enhancement (0000041472)** — VRRP Ping Virtual IP of Backup. For more information, see page105.
- **Enhancement (0000038652)** — Unauthenticated VLAN Access (Guest VLAN Access). For more information, see page 109.

- **Enhancement (0000011015)** — Cached Re-authentication (Hold State if Radius Server Unavailable). For more information, see page 110.
- **PC Phone/Authentication (PR_0000038652)** — When an IP phone is connected in tandem with a PC, the switch would not allow the PC user to be in an unauthenticated VLAN or authenticate using 802.1X, Web auth, or MAC authentication

Release K.14.48

The following problems were resolved in release K.14.48 (not a public release).

- **802.1X (PR_0000037816)** — 802.1X does not allow for authentication of new clients when the client-limit is reached; unauthenticated clients contribute to the client-limit. This fix gives authenticated users precedence over unauthenticated users. In addition, the relevant 'show' commands are updated to display clients in the unauthenticated state so the administrators will have the ability to see unintended users on a port.
- **802.1X (PR_0000044041)** — When a large number of 802.1X supplicants log off a single port simultaneously, the switch may reboot unexpectedly, logging a crash message similar to the following.

  Software exception at aaa802lx_util.c:2265 -- in 'm802lxCtrl', task ID = 0x84c1a10

- **Authentication (PR_0000017371)** — Unknown 802.1X, Web-, and MAC-Authentication clients take too long connect, causing very slow DHCP addressing.
- **Authentication (PR_0000045833)** — Some EAP requests are not properly handled by the switch.
- **Authentication (PR_0000046171)** — When a client is authenticated on a port with one authentication method, if the client is moved to a different port with a different authentication method, the switch correctly lists the client as being authenticated on the second port, but does not remove the client from the first port.
- **CLI (PR_0000008145)** — Counters for the following commands do not increment correctly when a TCP port is blocked by a NAS filter in a RADIUS-assigned ACL.

  ```
  show port-access authenticator clients <PORT-LIST> detailed
  show port-access mac-based clients <PORT-LIST> detailed
  show port-access web-based clients <PORT-LIST> detailed
  ```

- **CLI (PR_0000012407)** — Output from the CLI command **show port-access authenticator <port number> client details** shows the Frames In and Frames Out for each client to be exactly the same and it does not increment as it should. Workaround: Output from the CLI command **show port-access authenticator <port> session-counters** shows the Frames In and Frames Out incrementing correctly.
- **CLI (PR_0000043334)** — When the CLI config command **aaa port-access authenticator** is issued for a port that is part of a trunk, the error message is generic and does not let the user know the problem. This fix introduces a more specific error message.
- **Config (PR_0000040782)** — When an HP ProCurve Gigabit 1000Base-T Mini-GBIC (J8177C) is configured with the **speed-duplex auto-100** setting, that configuration is lost from both running and startup configurations after a switch reload.
- **COS (PR_0000046599)** — The switch reports incorrect Class Of Service (COS) information in the output of the command **show port-access auth <port>** when the default COS (value 255) is in effect.
- **Crash (PR_0000017707)** — The configuration of Web Authentication and connection of a PC into a switch port followed by an attempt to browse the Web will trigger a switch to reboot unexpectedly with a software exception.

- **Crash (PR_0000041445)** — When Web Authentication is in use, the switch may experience conditions that cause it to reboot unexpectedly with a crash message similar to the following.

```
Software exception at buffers.c:2231 -- in 'tHttpd', task ID = 0x80d25b0
```

- **Crash (PR_0000043188)** — Rarely, downloading a config file from a TFTP server to the switch may cause the switch to reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at hwBp.c:156 -- in 'tDcacheUpd', task ID = 0xa9835c0
```

- **Crash (PR_0000043538)** — When multiple 802.1X users try to authenticate simultaneously, the module or port bank may reset unexpectedly with messages similar to the following.

```
chassis: Slot B: Msg loss detected - no ack for seq #
chassis: Slot B: Lost Communications detected - Source Message System(50)
chassis: Slot B Slave ROM Tombstone: 0x13000601
Software exception at interrupts_bts.c:294 -- in 'tMsgCount', task ID = 0x4489bb1c
```

- **Crash (PR_0000043740)** — When switch ports are configured for both 802.1X authenticator and MAC-authentication, with different authenticated VLAN ID's for each, the switch may reboot unexpectedly with a software exception as they try to authenticate a client using both methods simultaneously. One of the following messages may be recorded by the switch crash log.

```
Software exception at portsecMaster_util.c:1088 -- in m8021xCtrl'
Software exception at portsecMaster_util.c:1093 -- in m8021xCtrl'
```

- **Crash (PR_0000043765)** — Switches performing port-access authentication may experience an unexpected reboot with a crash message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at radius_request.c:1472 -- in 'mRadius006', task ID = 0x8320
```

- **Crash (PR_0000043802)** — When GVRP is configured and the switch is learning GVRP VLANs through a trunk, if GVRP is disabled on the neighboring switch, or if the neighbor switch is reloaded, the switch will reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at vls_dyn_reconfig.c:2487 -- in 'mGarpCtrl', task ID = 0x83b9670
```

- **Crash (PR_0000044219)** — When the switch is configured for web-auth with client moves enabled using the CLI command **aaa port-access web-based <port-list> client-moves**, if a client is authenticated on one port and moves to another port (also configured for web-auth), the switch may reboot unexpectedly with a crash message similar to the following. Note that this problem was found and fixed on an internal software development build; symptoms in released software may vary.

```
Software exception at wma_client_sm.c:387 -- in 'mWebAuth', task ID = 0x8379a70
```

- **Crash (PR_0000044225)** — When multiple MAC-authentication clients attempt to log in to the switch with a RADIUS-assigned VLAN unknown to the switch, the switch may reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at radius_util.c:463 -- in 'mRadius006', task ID = 0x8306d60
```

- **Crash (PR_0000046643)** — With DHCP Snooping enabled on a VLAN, if a client requests a DHCP address and receives it from a trusted port, these changes can cause the switch to reboot unexpectedly:

  1. the client port is disabled
  2. the trusted port configuration is changed to be untrusted

3. the client port is re-enabled and the client requests a DHCP address, but the response comes from the now-untrusted port

The switch logs a message similar to the following.

```
Software exception at pmgr_util.c:1283 -- in 'mIpPktRecv', task ID = 0xa972cc0
```

- **DHCP Snooping (PR_0000046831)** — The switch forwards DHCP Discovery packets out untrusted ports.
- **Enhancement (PR_0000016657)** — Access Control Debug Logging changes have been made. For more information, see "Access Control Debug Logging" on page 112.
- **Enhancement (PR_0000042147, PR_0000042840)** — Port-Based Debug Logging Enhancement. For more information, see "Port-Based Debug Logging" on page 114.
- **Mini-GBIC (PR_0000044130)** — The HP ProCurve Gigabit-SX-LC Mini-GBIC (J4858C) does not transmit after a switch reboot or hot-swap when it is used in a dual-personality port.
- **Port Access (PR_0000017541)** — The switch allows an inherent configuration conflict; port-based 802.1X should not be allowed concurrently with Web and MAC authentication.
- **Port Access (PR_0000043432)** — CLI output from the command **show port-access authenticator** does not update the authenticated client list for local authentication clients.
- **Port Authentication (PR_0000042402)** — Configuration of 802.1X after MAC-Authentication will override the MAC-Auth logoff-period value. A previous fix (PR_0000010737) allowed the network administrator to see that all logoff timers on a port (802.1X, MacAuth, WebAuth) are functionally identical; i.e. writing a value to one will automatically write them all. This fix allows different timers to be used for different authentication methods.
- **RADIUS (PR_0000043940)** — With the Single Source IP Identity feature enabled, the "Radius-NAS-IP Attribute" sent by the switch is using the outgoing interface as the source address instead of the address defined in the **ip source-interface** configuration.
- **RADIUS Accounting (PR_0000043555)** — When the switch is configured for RADIUS accounting of commands (**aaa accounting commands stop-only radius**), and a user has logged on to the switch via telnet, the switch sends the incorrect calling-station-id AVP in the radius-accounting-request packet. The calling-station-id AVP is supposed to list the IP address of the host from which the user has connected to the switch.
- **sFlow (PR_0000015656)** — Outbound sampling using sFlow is not functioning.
- **TFTP (PR_0000046863)** — The switch experiences a loss of free memory each time a software image is downloaded via TFTP, unless there is a redundant management module installed.
- **Web Authentication (PR_0000016178)** — When a client connecting to the switch through Web Authentication enters the wrong credentials, the switch places the client in the unauth-vid and does not prompt for authentication retry. Once the port is in the unauthenticated state, only a reload of the switch allows for reauthentication.
- **Web Authentication (PR_0000017374)** — Following successful Web Authentication by a client, the browser redirect (to either the configured redirect URL or the client's home page) does not work.
- **Web Authentication (PR_0000017431)** — During Web Authentication login, the login progress pages are cached and the user is subjected to these cached pages when trying to navigate to other sites after successful authentication.
- **Web Authentication (PR_0000018047)** — A Web Authentication request may return a blank page.
- **Web Authentication (PR_0000018869)** — After redirection to the login page, and successful login using Web Authentication, the initial URL cannot be reached.
- **Web Authentication (PR_0000037786)** — Login progress pages provided during Web Authentication give the end-users an "Access Granted" page prior to completion of the network transition. Better dialogue with clearer instructions to end-users is implemented with this fix.

- **Web Authentication (PR_0000042390)** — The Web Authentication login page is no longer functional after there has been a configuration change in the DHCP range the switch uses for Web-auth.
- **Web Authentication (PR_0000043209)** — Following successful Web Authentication, the browser redirect does not work correctly; it omits the hostname from the redirect URL.

Release K.14.49

Software never built.

Release K.14.50

The following problems were resolved in release K.14.50 (not a public release).

- **Config (PR_0000037570)** — After using the CLI to assign a port in a VLAN number higher than 32, the configuration cannot be saved via the Menu interface.
- **Console Connectivity (PR_0000042248)** — The console port on a switch may get into a state where it appears to be unresponsive.
- **Enhancement (PR_0000048021)** —Support was added for the following products.

  J9310A - HP ProCurve 3500yl-24G-PoE+ Switch
  J9311A - HP ProCurve 3500yl-48G-PoE+ Switch
  J9312A - HP ProCurve 10-GbE 2-Port SFP+/2-Port CX4 yl Module
- **Event Log (PR_0000046782)** — When the switch detects an issue with PoE+ power, the event log message is now more informative. The old message `PSE detected. Port PoE disabled` is changed to `Possible bad FET/ PSE supplying PoE power - suggest configuring other end of link with 'no power'.`
- **PoE (PR_0000043773)** — The "MPS absent" counter does not increment when a PoE-powered device (PD) is removed from a switch port.
- **PoE (PR_0000044027)** — In a rare situation, the switch may erroneously display PoE Detection Status as "disabled" for some ports.
- **Savepower (PR_0000043096)** — This fix improves the event log messages when "savepower" is configured, and provides more detailed output from the **show savepower led** command.

Release K.14.51

The following problems were resolved in release K.14.51 (not a public release).

- **Config (PR_0000043984)** — The switch allows an inherent configuration conflict; the **rate-limit** and **service-policy** parameters should not be allowed concurrently on an interface.
- **Console (PR_0000001136)** — Rarely, the switch console may hang after a software image transfer to the switch. Workaround: **<Ctrl-C>** will restore the command prompt.
- **Counters (PR_0000048657)** — When a switch port is supplying more than 9.9 Watts of power to a port, the **show power brief** output truncates the displayed value. For example, the switch displays 10... instead of 10.3 W.
- **DHCP Snooping (PR_0000046276)** — With DHCP snooping enabled, a MAC-Authentication client whose session times out cannot reauthenticate.

- **IPv6 (PR_0000042273)** — The switch responds to LLDP requests with the first IPv6 address defined internally, which may be the link-local address. With this fix, the switch will advertise an IPv6 address that can communicate to remote sites.
- **IPv6 (PR_0000045773)** — IPv6 duplicate address detection (DAD) does not work properly in some topologies.
- **SSH (PR_0000046860)** — After a client public key is copied to the switch via TFTP, if the user uses SSH to connect to the switch, when the SSH session is closed the switch reboots unexpectedly with a software exception message.
- **TFTP (PR_0000046063)** — When the management VLAN is changed from the default (VLAN 1), the switch does not respond to TFTP requests.
- **Transceivers (PR_0000045170)** — The J8437A X2-SC LR Optic (transceiver) continues to transmit after the interface is disabled, which causes the far end to think the link is still up.
- **Transceivers (PR_0000045482)** — Some J9152A SFP+ LRM transceivers do not turn on the laser after the switch reboots. Workaround: remove, then re-insert the transceiver.
- **Unauthenticated VLAN (PR_0000010533)** — The switch allows an inherent configuration conflict; an unauthenticated VLAN (**unauth-vid**) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an **unauth-vid** for the **aaa port-access authenticator** and **aaa port-access web-based** or **aaa port-access mac-based** functions. Software versions that contain this fix will not allow this configuration conflict at the CLI. *Existing configurations will be altered by this fix*, and an error will be reported at the switch CLI and event log.

  Best Practice Tip: 802.1X should not have an unauthenticated VLAN setting when it works concurrently with Web-based or MAC-based authentication if the unauth-period in 802.1X is zero (the default value). Recall that the unauth-period is the time that 802.1X will wait for authentication completion before the client will be authorized on an unauthenticated VLAN. If 802.1X is associated with an unauthenticated VLAN when the unauth-period is zero, Web- or MAC-auth may not get the opportunity to initiate authentication at all if the first packet from the client is an 802.1X packet. Alternatively, if the first packet sent was not 802.1X, Web- or MAC-auth could be initiated before 802.1X places the user in the unauthenticated VLAN and when Web- or MAC-auth completes successfully, it will be awaiting traffic (to enable VLAN assignment) from the client but the traffic will be restricted to the unauthenticated VLAN, and thus the client will remain there.

  If a MAC- or Web-based configuration on a port is associated with an unauth-VID, and an attempt is made to configure an unauth-VID for 802.1X (**port-access authenticator**), the switch with this fix will reject the configuration change with a message similar to one of the following.

  Message 1 (when an unauth-vid config is attempted on a port with an existing Web- or MAC-auth unauth-vid):

  ```
  Configuration change denied for port <number>. Only Web or MAC authenticator can have
  unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
  Please disable Web and MAC authentication on this port using the following commands:
  ```

  no aaa port-access web-based <PORT-LIST> or
  no aaa port-access mac-based <PORT-LIST>

  ```
  Then you can enable 802.1X authentication with unauthenticated VLAN. You can re-enable
  Web and/or MAC authentication after you remove the unauthenticated VLAN from 802.1X.
  Note that you can set unauthenticated VLAN for Web or MAC authentication instead.
  ```

  Message 2 (when an unauth-vid config is attempted on a port with an existing 802.1X unauth-vid):

  ```
  Configuration change denied for port <number>.Only Web or MAC authenticator can have
  unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
  Please remove the unauthenticated VLAN from 802.1X authentication on this port using
  the following command:
  ```

  no aaa port-access authenticator <PORT-LIST> unauth-vid

  ```
  Note that you can set unauthenticated VLAN for Web or MAC authentication instead.
  ```

Message 3:

```
Configuration change denied for port <number>. Only Web or MAC authenticator can have
unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
Please use unauthenticated VLAN for Web or MAC authentication instead.
```

Event log message when the configuration is changed:

```
mgr: Disabled unauthenticated VLAN on port <number> for the 802.1X.
Unauthenticated VLAN cannot be simultaneously enabled on both 802.1X and Web or MAC
authentication.
```

- **Virus Throttling (PR_0000039749)** — A port that receives IPv6 traffic and is configured for virus throttling can cause high CPU utilization on the switch.

Release K.14.52

The following problems were resolved in release K.14.52 (not a public release).

- **802.1X (PR_0000047025)** — After the switch reboots and before IP communication is initialized, the switch accepts authentication requests from 802.1X clients. Because the switch cannot communicate with the RADIUS server yet, it sends EAP-Failure notifications to the client, which causes client authentication to fail.
- **BPDU Protection (PR_0000047748)** — This fix corrects the output of an SNMP query. Before the fix, the switch might incorrectly respond that BPDU protection is disabled on a port, when in fact it is enabled and functioning properly.
- **Config (PR_0000049009)** — A configuration file that contains the **savepower led** or **savepower port-low-pwr** parameters cannot be downloaded to the switch. The download fails with a `Corrupted download` file message.
- **Crash (PR_0000043167)** — When using TFTP with "octet" mode to upload the switch's configuration file, the switch may reboot unexpectedly with a message similar to the following.

```
Software exception at hwBp.c:156 -- in 'eDevIdle', task ID = 0xabeb240
-> MemWatch Trigger: Offending task 'tTftpDmn'.
Offending IP=0x1cb174
```

- **Distributed Trunking (PR_0000045026)** — When a server is connected to a pair of switches via distributed trunking, the switches do not respond to communication attempts (for example ping or telnet) from the server.
- **Distributed Trunking (PR_0000048802)** — After powering down a switch participating in a distributed LACP trunk, the remaining switch does not take over the conversations previously running through the offline switch. Workaround: Do not power down a switch running Distributed Trunking. If a reload is required, first unplug the Distributed Trunk links from the switch, wait at least one minute, then unplug the Inter-Switch Connection (ISC), then reload or power down the switch.
- **IGMP (PR_0000018494)** — IGMP joins may cause multicast streams to flood, briefly, across the VLAN.
- **IP Communication (PR_0000042790)** — A very busy switch may cease all IP communication when the CLI command **show tech route** is executed. Messages similar to the following may be seen in the event log when this occurs.

```
W <date> <time> 00436 NETINET: 1 route entry creation(s) failed.
W <date> <time> 00075 system: Out of pkt buffers; miss count: 0
```

- **IP Communication (PR_0000043121)** — Execution and subsequent interruption of the CLI command **show tech route** during a vulnerability scan negatively affects IP communication.
- **Port Communication (PR_0000043048)** — The switch will not allow a port to link if the MDIX-MODE is set to MDI or MDIX (only the **auto-MDIX** setting will allow link).

- **Port Connectivity (PR_0000038601)** — The time between a port coming up and that port being online and passing traffic varies, and at times, may be extended to over a minute.
- **QoS (PR_0000039751)** — Strict outbound queuing is being enforced on trunk ports; when traffic is egressing (sent out of) a trunk port on multiple queues, the higher priority queues will starve out lower priority queues when oversubscribed.
- **Rate Limiting (PR_0000047195)** — HP ProCurve ONE environment protects the network from non-ONE applications by imposing rate limits on the ONE Services zl module ports. In some cases, a demonstration activation license for a ONE application is not interpreted correctly as a valid ONE activation license and the rate limits are imposed.
- **SNMP (PR_0000045869)** — When a large number of SNMPSET commands (on the order of 100 commands) are sent to the switch, at some point the switch runs out of room to store those entries. When the switch's memory limit is reached it gives this error message: `snmp: event 1997; events file too big; record not written`. This fix increases the available memory to allow the switch to accept up to 380 SNMPSET commands.
- **SNTP Authentication (PR_0000048588)** — With SNTP authentication disabled, the switch sends extra, unnecessary authentication information in the SNTP request packet.
- **STP (PR_0000017189)** — When the switch is running in RSTP-mode (through the use of the CLI configuration command **spanning-tree force-version rstp-operation**) and MSTI settings are still present in the switch, a TCN is triggered when the MSTI settings are modified or removed.
- **UDLD (PR_0000047414)** — When UDLD is enabled, communication with the switch might be inconsistent, affecting the switch response to ping, telnet, 802.1X requests, SNMP requests, and SNTP packets.
- **VRRP (PR_0000018777)** — In a VRRP topology with two VRRP routers configured as Backup VRRP routers of the same priority, a simultaneous reboot of the two VRRP routers may lead to a situation where no VRRP router becomes the Master. This fix enhances VRRP functionality for skew time implementation as per RFC 3768.
- **Web Authentication (PR_0000048491)** — The Web Authentication login page is not presented to Web Authentication clients.

Release K.14.53

The following problems were resolved in release K.14.53 (not a public release).

- **CLI (PR_0000040869)** — A QoS policy that is applied to a switch interface cannot be removed with the CLI.
- **CLI (PR_0000047545)** — The CLI command **no telnet-server** is not saved in the config file.
- **Crash (PR_0000047161)** — With QinQ S-VLAN mode enabled, the switch may reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

  ```
  Software exception at vls_demux.c:880- in 'eDrvPoll', task ID = 0x61fe800
  ```

- **Crash (PR_0000047852)** — After deleting a VLAN that had been running PIM-sparse mode, if PIM-dense mode is enabled on a different VLAN, the switch may reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

  ```
  Software exception at pim_dm_init.c:1773 -- in 'mSnmpCtrl', task ID = 0xa93c440
  ```

- **DHCP Snooping (PR_0000048426)** — With DHCP Snooping enabled, a client DHCP request is forwarded out untrusted ports.
- **Event Log (PR_0000043041)** — When the switch downgrades a port from Gigabit to 10/100 operation, the resulting event log "FFI" message is displayed twice.

- **Guaranteed Minimum Bandwidth (PR_0000042500)** — The switch does not allow Guaranteed Minimum Bandwidth (GMB) to be configured on port L24. Also, a configuration file with GMB on port L24 fails to load onto the switch.
- **IP Connectivity (PR_0000046280)** — After updating software, the hostname is removed from the configuration and the switch does not respond to SSH requests.
- **OSPF (PR_0000045110)** — With OSPF routing and OSPF traps enabled, the switch's available memory decreases over time.
- **SNMP (PR_0000046735)** — Event log messages of type "Info" are sent as traps even after applying the configuration command **snmp-server host <IPaddress> <community> not-info**.
- **SNTP (PR_0000048717)** — The switch does not ensure the VLAN is up before sending SNTP requests, which can result in SNTP timeouts.
- **SSH (PR_0000045158)** — SSH login to the switch might fail.
- **SSH (PR_0000046259)** — The output of a CLI **show** command may have truncated lines, when the **show** command is executed via an SSH login and the output is very large (on the order of 2 KB).
- **VRRP (PR_0000049259)** — In some situations the VRRP Virtual IP does not respond to ping. This fix refines the enhancement introduced in K.14.47 with PR_0000041472.

Release K.14.54

The following problems were resolved in release K.14.54 (not a public release).

- **CLI (PR_0000049955)** — The output of **show tech route** does not include all the information it is intended to provide.
- **CLI Help (PR_0000048102)** — The debug help text (when the user types **debug ?**) offers some invalid parameters.
- **Enhancement (PR_0000044183)** — Display interface configuration enhancement. For more information, see “Display Configuration of Selected Interface” on page 114.
- **Enhancement (PR_0000045649)** — Post-logon banner enhancement. For more information, see “Post-Logon Banner” on page 120.
- **Enhancement (PR_0000045711)** — Web authentication message enhancement. For more information, see “Web Authentication Message” on page 123.
- **Enhancement (PR_0000045749)** — Module reload enhancement. For more information, see “Module Reload” on page 127.
- **Enhancement (PR_0000045752)** — User-configurable per-port MAC address enhancement. For more information, see “User-Configurable Per-Port MAC Address” on page 128.

Release K.14.55

The following problems were resolved in release K.14.55 (not a public release).

- **BootROM (PR_0000039743)** — When software containing a boot ROM update is copied to the primary flash of the switch and the switch is reloaded into the primary image, the boot ROM does not successfully update. Workaround: Copy software with boot ROM update to secondary, and execute the CLI command **boot system flash secondary** to load the secondary image.

- **CLI (PR_0000050078)** — When a PoE power supply is hot-swapped into a Switch 5400zl or 8200zl, the output of the CLI command **show system power** always lists the power supply as being 120 V, 875 W, even if it is a different voltage/wattage power supply.
- **CLI (PR_0000050088)** — If the user removes an interface module from the switch configuration (for example with the command, **no module 1**), an SNMP link-change trap configuration for ports on that module is truncated instead of removed from the configuration. For example, the configuration **no snmp-server enable traps link-change A1-A2** is truncated to **no snmp-server enable traps link-change**, which is an invalid configuration. If the user saves that configuration to a server, the config file cannot be successfully downloaded to the switch because of the incomplete command.
- **CLI (PR_0000051293)** — The switch allows an invalid command **no reload module**, which when entered causes the specified module to reload immediately.
- **Config (PR_0000046578)** — An IP BOOTP gateway configured on subnet zero is not displayed in the startup or running configuration file. The gateway is used correctly by the switch; this is a configuration display issue only.
- **Crash (PR_0000051910)** — With software versions K.14.53 and K.14.54, SSH login to the switch might fail, and the switch may reboot unexpectedly with a message similar to the following.

```
NMI event SW:IP=0x00f64f88 MSR:0x02029200 LR:0x00f654dc cr:0x20000000
sp:0x05337598 xer:0x00000000 Task='tTelnetOut2' Task ID=0xa903000
```

- **Crash Messaging (PR_0000049806)** — Beginning with K.14.38, a coredump file is not generated when the switch crashes.
- **Enhancement (PR_0000018427)** — Multicast ARP support enhancement. For more information, see page 128.
- **File Transfer (PR_0000048178)** — While loading switch software via Secure Copy (SCP) or TFTP, the switch can be rebooted by the user before the software file load completes.
- **LLDP (PR_0000048124)** — The LLDP Port VLAN ID TLV is incorrectly advertised as 0 for Trunked ports.
- **Module Crash (PR_0000043280)** — With IP routing and QinQ enabled, a switch module may reboot unexpectedly with a message similar to the following.

```
00374 chassis: Ports C: Lost Communications detected - Heart Beat Lost
```

- **PIM (PR_0000050672)** — Fragmented PIM packets are not correctly routed by the switch.
- **SNMP (PR_0000046906)** — Responses to SNMP queries on a switch configured with trunk groups are slow, which can lead to SNMP polling failures.
- **TACACS (PR_0000047886)** — When a TACACS server is not available, the switch waits 40 seconds or more before the TACACS request is timed out and the configured secondary authentication method is tried. By default, the timeout should take 5 seconds.
- **Unauthenticated VLAN (PR_0000045072)** — An unauthenticated VLAN cannot be configured for 802.1X authentication, when another authentication method is also in use on a port. This fix also adds the **unauth-period** parameter for MAC authentication.

Release K.14.56

The following problems were resolved in release K.14.56 (not a public release).

- **Authentication (PR_0000043924)** — The switch responds with invalid PEAP packets when the RADIUS server request includes optional EAP TLVs, resulting in authentication failure.

- **CLI (PR_0000044704)** — The switch does not properly adjust terminal size display, if the user telnets to the switch and then changes the terminal size. This can cause the username to display when the password is requested, instead of a blank field.
- **Counters (PR_0000048734)** — After clearing counters on all ports with the command **clear statistics global**, if the counters on a single port are subsequently cleared, counters on other ports revert to their pre-cleared values.
- **LLDP-MED (PR_0000018681)** — LLDP-MED responses from a device connected to the switch are stored in the wrong order, which causes errors when the user uses "snmpwalk" to see the stored values on the switch.
- **LLDP-MED (PR_0000050798)** — In some cases the LLDP-MED inventory for an attached IP phone is not properly received or stored by the switch.
- **UDLD (PR_0000050402)** — With UDLD enabled, a trunk that uses fiberoptic transceivers stops forwarding traffic after a switch reboot.
- **VRRP (PR_0000042589)** — When the switch is very busy (for example, when downloading a very large config file), VRRP may experience multiple failovers back and forth to the backup router.
- **VRRP (PR_0000052012)** — VRRP hello packets are sent later than the configured **advertisement-interval**, which can result in failover to the backup router. This issue is in software versions K.14.52 - K.14.55.
- **VRRP (PR_0000052019)** — VRRP skew timers do not match IETF specifications, which can result in failover to the backup router. This issue is in software versions K.14.52 - K.14.55.

Release K.14.57

The following problems were resolved in release K.14.57 (not a public release).

- **Authentication (PR_0000054344)** — The request sent from switch to RADIUS server truncates the username to 16 characters, which causes authentication failure if the username is longer than 16 characters.
- **Authentication (PR_0000054384)** — In some situations an unauthenticated client can access the authenticated VLAN.
- **DHCP (PR_0000002817)** — When the switch is acting as a DHCP relay agent, it uses UDP port 68 as the source for sending messages to the server. This fix changes the UDP source port for such communication to port 67.
- **Management (PR_0000054089)** — In software versions K.14.54 - K.14.56, initiating a management session to the switch causes the switch's available memory to decrease.
- **SSH (PR_0000051551)** — If an SSH session is closed during a large file transfer, the session cannot be re-opened.
- **SSH (PR_0000052970)** — The output of a CLI **show** command may have truncated lines, when the **show** command is executed via an SSH login and the output is very large (on the order of 2 KB). This improves the original fix in K.14.53 (PR_0000046259).
- **Stacking (PR_0000053271)** — The CLI command **no stack** does not disable stacking.

Release K.14.58

Software never built.

Release K.14.59

The following problems were resolved in release K.14.59 (not a public release).

- **802.1X (PR_0000038874)** — When using 802.1X in client mode, the command **aaa port-access authenticator 1 client-limit 2** should allow two clients to authenticate on that port. After one client is removed and the timeout period has passed, the switch does not allow a new second client to authenticate.
- **802.1X (PR_0000047205)** — Cached reauthentication does not work with Windows XP running Service Pack 3.
- **CLI (PR_0000051739)** — The "alias" command configuration is removed from the config file upon reboot. Also, the output of **show alias** does not include the name of the alias.
- **Crash (PR_0000046562)** — If the user removes the IP address from a VLAN on a switch configured for PIM-SM, when the user reconfigures an IP address on that VLAN the switch may reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

  ```
  Software exception at pim_sm_util.c:2430 -- in 'mPimsmCtrl', task ID = 0xa90ba40
  ```

- **Crash (PR_0000046565)** — In some situations the switch may reboot unexpectedly with a message similar to the following.

  ```
  Software exception at mldFilteredGroup.c:235 -- in 'mMLD', task ID = 0xa968a80
  -> MldFilteredGroup_DeleteGroup group does not exist.
  ```

- **Crash (PR_0000047202)** — If a large configuration or switch software file is downloaded to the switch when the DHCP lease timer expires, the transfer will fail and the switch might reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

  ```
  Software exception at svc_timers.c:820 -- in 'mDHCPClint', task ID = 0x5d79880
  ```

- **Crash (PR_0000048592)** — With meshing enabled, if the switch receives a packet destined to a MAC address with certain parameters the switch might reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

  ```
  Software exception at bttfHwUtil.c:798 -- in 'eDrvPoll', task ID = 0x61fe800
  ```

- **Crash (PR_0000049154)** — In software versions K.14.52 - K.14.58, some situations related to IGMP-learned MAC addresses combined with a MAC address learned on an interface module can cause the switch to reboot unexpectedly with a message similar to the following.

  ```
  Software exception at bttfSlaveLearn.c:1691 -- in 'mAdMUpCtrl'
  ```

- **Crash (PR_0000049919)** — A rare situation related to source port filtering can cause the switch to reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

  ```
  Software exception at bttfDma.c:410 -- in 'tDevPollTx', task ID = 0xa9a1780
  ```

- **Crash (PR_0000050090)** — In some situations, attempting to delete a non-existent VLAN from the switch configuration might cause the switch to reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

  ```
  Software exception at vls_util.c:1380 -- in 'mMTM', task ID = 0xa967200
  ```

- **DHCP Snooping (PR_0000049563)** — The switch forwards DHCP packets when DHCP Snooping is configured globally but not on any VLANs.

- **DIPLD (PR_0000051983)** — A switch running Dynamic IP Lockdown (DIPLD) and DHCP Snooping has these two issues. If a port is part of multiple DHCP snooping-enabled VLANs and IP Lockdown is enabled on that port, removing that port from one VLAN disables IP Lockdown on all VLANs. Also, if a port is part of multiple DHCP snooping-enabled VLANs and IP Lockdown is enabled on that port, removing DHCP snooping on one VLAN disables IP Lockdown on all VLANs. This fix resolves both issues.
- **Dynamic ARP Protection (PR_0000050543)** — The switch reserves an incorrect amount of internal memory when Dynamic ARP Protection is enabled.
- **Enhancement (PR_0000018479)** — Longer usernames and passwords are now allowed, and some special characters may be used. For more information, see "Username and Password Size Increase" on page 129.
- Enhancement (PR_0000045707) — The tilde character is now allowed in TACACS+ and RADIUS encryption keys. For more information, see "Support for the Tilde (~) Character in TACACS+ and RADIUS Keys" on page 131.
- Enhancement (PR_0000052732) — Enhancement to increase the MAC Authentication Client Limit to 256. For more information, see "Increase MAC Auth Client Limit to 256" on page 134.
- Enhancement (PR_0000052801) — Categorize CLI Return Messages enhancement. For more information, see "Categorize CLI Return Messages" on page 134.
- **IGMP (PR_0000052737)** — With Forced Fast-Leave disabled (which is the default), upon receipt of a "leave" message from a client, the switch sends a Group Specific Query with a Max Response Time of zero seconds, which is not a valid value.
- **OSPF (PR_0000048868)** — When an OSPF area is reconfigured from NSSA to normal, the NSSA default route is retained by the switch instead of being immediately removed.
- **Routing (PR_0000049455)** — In certain rare situations with a large number of routes and multicast routing enabled, the switch CPU utilization might remain at 100%, leading to sluggish response and possible loss of multicast routes.
- **Services Module (PR_0000045163)** — The ProCurve ONE zl module CLI does not respond during heavy traffic conditions.
- **Services Module (PR_0000048246)** — If the switch configuration includes several hundred VLANs, the applications on a ProCurve ONE zl module may fail to start properly. When this happens, the "Module Status" LED will continue to blink green and will not transition to the normal solid green state. Also, the output of the **show services <slot>** command will display "booted" in the "Current Status" field and will not transition to the normal "running" status.
- **SNMP (PR_0000044963)** — In some rare situations, SNMP commands from a ProCurve ONE application might cause switch memory to decrease.
- **SNMP (PR_0000045943)** — When using SNMP to initiate a TFTP "get" of a file from the switch, if the requested file does not exist, the switch responds with a vague error message. This fix implements meaningful error messages in that situation.
- **SNMP (PR_0000046848)** — SNMP traps are sent to the in-band VLAN, even if configured to send SNMP traps to the Out-of-Band Management (OOBM) interface. This fix adds an option in CLI to specify OOBM as the trap destination.
- **SNMP (PR_0000050956)** — SNMP traps contain hexadecimal characters instead of valid event log messages.
- **Syslog (PR_0000046914)** — Syslog messages from the Out-of-Band Management (OOBM) port have a source IP of the inband VLAN, instead of the OOBM interface.
- **TELNET (PR_0000047906)** — A telnet session to the switch is not dropped when the IP address to which the telnet session connected is removed from the interface.
- **TFTP (PR_0000049655)** — After enabling Secure Copy (SCP) which automatically disables TFTP, the switch continues to send information via TFTP.

- **Trunking (PR_0000038646)** — The switch does not allow generic trunks on the ONE zl modules.

Release K.14.60

The following problems were resolved in release K.14.60.

- **Authentication (PR_0000054835)** — After the first client is authenticated on a port, subsequent clients that fail Web-authentication on that port can access the authorized VLAN.
- **Authentication (PR_0000055580)** — After the first client is authenticated on a port, subsequent clients that are authenticated on that port are incorrectly placed on the same authorized VLAN as the first client, instead of being placed on their appropriate VLANs.
- **Banner MOTD (PR_0000054833)** — The switch experiences a loss of free memory when a login banner is configured.
- **CLI (PR_0000050756)** — When the user presses **<Ctrl>c** to cancel the output of a previously-issued command, in some cases the **<Ctrl>c** does not appear to have any effect, and the switch displays the remaining output of the previous command.
- **File Transfer (PR_0000039190)** — A configuration file that has a QoS policy applied to a VLAN (**vlan <vlan-id> service-policy <policy-name> in**) cannot be downloaded to the switch.
- **IP Communication (PR_0000053603)** — The switch responds to an ARP request received on one VLAN but sent from a different VLAN. This situation can occur when a client's port is moved from one VLAN to another, and the client sends an ARP request from an IP address on the original VLAN.
- **IP Communication (PR_0000053861)** — The switch is unable to telnet or ping to supernetted IP addresses, and supernetted IP addresses cannot be configured on the switch.
- **Routing (PR_0000053115)** — With the VLAN MAC Address Reconfiguration feature enabled, routed packets are forwarded at very slow rates if the switch's route table has a large number of entries.

Release K.14.61

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.61.

Config (PR_0000041014) — When the CLI command **no module** is used to remove a module's configuration, the switch does not clear corresponding aaa configuration as it should.

Crash (PR_0000052464) — A switch that has a large number of ACLs applied by the Identity Driven Manager (IDM) application might reboot unexpectedly with a message similar to the following.

```
Software exception at enDecode.c:54 -- in 'midmCtrl', task ID = 0xa946380
-> out of memory!
```

DHCP (PR_0000054749) — When the switch acts as a DHCP relay agent, it erroneously removes the "end" option (code 255) from DHCP packets.

DIPLD (PR_0000052518)—With Dynamic IP Lockdown enabled, there is no communication between clients on the switch.

Event Log/DIPLD (PR_0000049068)— When Dynamic IP Lockdown (DIPLD) drops a packet, the resulting event log `access denied` message has missing and incorrect information.

PIM - (PR_0000054424) —When a multicast source is connected to a VLAN with multiple IP address ranges (a "multinetted VLAN"), and the multicast source is configured with an IP address in one of the secondary IP address ranges, the multicast streams are not forwarded by the switch.

sFlow (PR_0000012123) — The switch does not allow sFlow to be configured on a mirror port.

sFlow (PR_0000041583) —The switch does not send VLAN tag information in sFlow data.

SNMP (PR_0000053686) — On a switch with a separate out-of-band management port, disabling web management causes SNMP queries to fail, when those queries are sent to the switch's in-band VLAN IP address. This symptom appears after web management is disabled and the switch is subsequently rebooted.

SNMP/Config (PR_0000039221) — The switch can misinterpret the community name as if it were a trap level, in the **snmp-server host** command. This fix modifies the command with keywords **community** and **trap-level**. The new command syntax is as follows.

> **snmp-server host <ip addr> [community <community string>] [trap-level <none | all | not-info | critical | debug>] [informs].**

Switch Hang (PR_0000055888) —Updating switch software from K.12 or K.13 to K.14.03 - K.14.60 might, in a very small number of cases, result in the switch failing to boot after update. The system will hang after displaying the `Decompressing...done` message, and will not recover.

Release K.14.62

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.62.

CLI (PR_0000052751) — If a specific MAC address (MACx) exists on more than one physical port (with each port in a different VLAN), the output of the command **show mac-address MACx** lists that MAC address on only one of the ports.

Enhancement (PR_0000052738) — Adds VLAN information to the output of the **show mac-address** commands. For more information, see “Show MAC with VLAN” on page 137.

Enhancement (PR_0000053047) — Adds a global configuration option that allows each VLAN to have a multicast filter. For more information, see “Block Unknown Multicast” on page 139.

Enhancement (PR_0000054042)— Adds the ability to monitor egress queues for dropped packets when QoS is configured. For more information, see “Outbound Queue Monitor” on page 143.

Enhancement (PR_0000054055) — This enhancement provides the ability to display OSPF neighbor timer information. For more information, see “Show OSPF Neighbor Timers” on page 144.

Enhancement (PR_0000054183)— The user can now disable the IP addresses on specified VLANs, without deleting the configured IP addresses. For more information, see “IP Enable/Disable for All VLANs” on page 144.

Release K.14.63

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.63.

CLI (PR_0000010193)— Debug commands for VRRP and OSPF are available when a premium license is not installed on the switch.

CLI (PR_0000046858)— The switch does not use the specified **startup-default** configuration file when the user types **reload**. If the user issues the **reload at** or **reload after** command, the specified **startup-default** file is correctly used. This fix also adds a warning message when the user issues the **startup-default** command.

CLI (PR_0000047495) — With the same trap receiver configured for multiple SNMP community names, if the user attempts to delete that trap receiver from any of the SNMP community names with the CLI command **no snmp-server host <ip-address> <community-name>**, the trap receiver that is deleted is always the trap receiver for the first configured SNMP community.

CLI (PR_0000048578)— The **<Ctrl-c>** break sequence does not work while the user is creating a custom login banner.

CLI (PR_0000050554) — The **debug acl** command is not available.

Console (PR_0000042791) — The output of **show interfaces** can be slightly different from switch to switch, depending on each switch's configuration. For example, for large values the counters might include commas in one case and not display commas in another case.

Counters (PR_0000048732)— The output of **show interfaces <port> hc** does not display the counters in hexadecimal as it should.

Counters (PR_0000048733) — The output of **show interfaces** has commas for large values in some, but not all fields. This fix makes the display consistent.

Crash (PR_0000038431) — When the Web Management Interface is used for port security configuration of 44 or more ports concurrently (Security > Port Security > Select 44 ports > click on 'Set Security Policy for the Selected Ports') the switch will reboot unexpectedly with a message similar to the following.

```
PPC Bus Error exception vector 0x300: Stack-frame=0x033ace80
HW Addr=0x37392c38 IP=0x0047ade0 Task='tHttpd' Task ID=0x33ad408
fp: 0x0000001c sp:0x033acf40 lr:0x
```

Crash (PR_0000041777) — If a configuration file with the entry **power-over-ethernet redundancy n+1** is downloaded to the switch, the switch will reboot unexpectedly with a message similar to the following.

```
PPC Data Storage (Bus Error) exception 0x300: esf=0x083a5570 addr=0xc3d2e1f0 ip=0x00113424
Task='mftTask' tid=0x83a69d0 fp=0x69696969 sp=0x083a5630 lr=0x001136
```

Crash (PR_0000056315)— From the Web interface of a commander switch, if the user removes a stack member and then tries the close-up view, the switch might reboot unexpectedly with a message similar to the following.

```
Invalid Instruction Exception number: 0x00000004HW Addr=0x434f535c IP=0x434f535c
Task='InetServer' Task ID=0xa6e2b80 fp: 0x434f535f sp:0x03129058 lr:0x00f224
```

Enhancement (PR_0000040979)— The **entry-count** parameter is added to these two commands: **show access-list** and **show policy**. When either of those commands is used with the **entry-count** parameter, the switch displays the number of configured class, policy, and ACL entries.

Event Log (PR_0000049520)— For some event log entries, the VLAN ID (VID) is not properly displayed if the VID has more than one digit.

Event Log (PR_0000050999)— If the CLI command is issued to download software to the switch, and during that download an SNMP request to download software is sent to the switch, the resulting error message is garbled.

Mirroring (PR_0000015825)— Remote mirroring and certain source/destination IP address combinations do not function properly; the remote destination switch does not copy the traffic to the mirror (exit) port.

MSTP (PR_0000045597) — If the user configures the path cost for a port in an MSTP instance, and then configures a priority for that same port in that MSTP instance, the switch changes the path cost back to the default value (auto). Workaround: configure the priority first, then configure the path cost. This issue is seen with MSTP instances only; configuring path cost and priority for ports in the CIST works properly.

OSPF (PR_0000040435)— If the switch is configured as an OSPF Area Border Router (ABR) with a Loopback 0 address assigned to area 0.0.0.0, the switch does not exchange inter-area routes after the last physical interface in area 0.0.0.0 goes down.

OSPF (PR_0000046029) — If there are routers in an OSPF area that do not support "demand circuits", virtual links (which are treated as demand circuits and should stop LSA aging) cause the LSAs to age out, causing SPF recalculation and periodic route flapping.

Port Connectivity (PR_0000050635) — When 7-meter Direct Attach Cables (J9285B) connect two switches, if one of the switches is rebooted, the connected ports might begin to toggle offline/online repeatedly.

Routing (PR_0000052349)— When a destination host does not respond, the switch sends the wrong ICMP message (`network unreachable` instead of `host unreachable`).

sFlow (PR_0000039269) — When sFlow is enabled on a trunk port and one of the trunk ports is disabled, the switch does not consistently send port counter data to the sFlow server.

sFlow (PR_0000049710) — During times of high traffic, the dropped samples counter displayed by **show sflow <port#> sampling-polling** is not updated.

TACACS (PR_0000052495)— If the switch is configured to use TACACS for telnet access and the TACACS timeout is configured for a value greater than 75 seconds, the switch waits much longer than 75 seconds before timing out the TACACS request.

Unauthenticated VLAN (PR_0000051515)— Using SNMP, the switch allows an inherent configuration conflict; an unauthenticated VLAN (unauth-vid) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an unauth-vid for the aaa port-access authenticator and aaa port-access web-based or aaa port-access mac-based functions. As with PR_0000010533, this fix will alter existing configurations. Please see the PR_0000010533 writeup (in K.14.51) for complete details.

Web Authentication (PR_0000042284)— When an EWA server is used for Web authentication, authentication is successful but custom graphics are not displayed.

Web Management (PR_0000044397) — Using the Web interface, the close-up view of stack members might not display if the commander is configured for SSL-only access. Also, if both the commander and member are configured for SSL-only access, connection to the stack member fails.

Release K.14.64

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.64.

Banner MOTD (PR_0000053198) —When using TACACS for telnet authentication, if a banner MOTD is longer than four lines, the first four lines of the banner are not visible on the screen.

Crash (PR_0000047516) — In rare situations with LACP enabled, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception at interrupts_bts.c:325 -- in 'fault_handler',
task ID = 0x60
-> Master Induced Crash. IGNORE!
```

Crash (PR_0000050103) — The switch allows setMIB commands to create invalid configurations, which might cause the switch to reboot unexpectedly when the user issues the **show running-config** command, with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at cli_xlate.c:5340 -- in 'mSess1', task ID = > 0xa924e00
```

Crash (PR_0000054005) — If an SFP+ transceiver or cable is present in the switch and the menu interface is used to make port or trunk configuration changes, the switch might reboot unexpectedly with a message similar to the following.

```
Access Violation - Restricted Memory
Exception number: 0xdead0000
HW Addr=0x3131393e IP=0x00002670 Task='mSess1' Task ID=0xa930640
fp: 0x05216200 sp:0x038ac7f0
```

File Transfer (PR_0000054790)—Switch software cannot be updated via HTTPS.

IP Communication (PR_0000053547)— With both a management VLAN and connection-rate filtering (virus throttling) configured, when a host on one virus-throttled port attempts to communicate with a host on a different virus-throttled port, the switch sends erroneous `destination unreachable` ICMP packets. However, the communication succeeds.

LEDs (PR_0000048829)— Although the event log reports an `Unrecoverable fault on PoE controller`, the switch LEDs do not indicate any problem.

OSPF (PR_0000055768) — After 255 topology changes, the next OSPF topology change resets the Shortest Path First (SPF) counter to 1 instead of incrementing to 256.

PIM-SM (PR_0000050032) — The switch logs erroneous `No pim neighbor on vid <VLAN-ID>, cannot send joinprune packet` messages. The event log messages are the only problem; PIM-SM functions properly.

PoE (PR_0000053516)— If a faulty PoE+ power supply is installed in the zl Power Shelf, the switch does not properly indicate that the power supply is bad. Instead, the switch displays `0W /Connected` in the **show power-over-ethernet** output. With this fix, a) the command output displays `0W /Connected - Faulted`, b) an event log message is generated: `Ext Power Supply <power-supply-number> measured out of spec or is faulty. Please change or contact support.`, and c) the Power Supply Status LED flashes orange.

PoE (PR_0000055223)— In some cases the PoE controller fails self-test, after software attempts to update the controller firmware.

Port Filters/OSPF (PR_0000048162) — Layer 2 filters on one port may break OSPF/VRRP Adjacency on another port in the same VLAN. This PR_0000048162 improves the original fix (PR_0000012665) documented in K.13 software (K.13.66).

QoS (PR_0000040868) —After configuring a default class in a classifier-based QoS policy, the command **no default-class** does not delete the default class.

QoS (PR_0000054917)— On a switch configured to use DSCP (command **qos type-of-service diff-services**), if one of the default DSCP policies is disabled and a lower-precedence QoS policy is applied (for example VLAN QoS), that new QoS policy is not used until the switch is rebooted. Workaround: disable DSCP on the switch so that the default policies are not used (command **no qos type-of-service diff-services**), or reboot the switch.

Web Management (PR_0000054861) —The Web "device view" of a switch shows the power supply status as green for all installed internal power supplies, even if a power supply is installed with no power cord connected.

Release K.14.65

Status: Released and fully supported and posted on the Web.
The following problems were resolved in software version K.14.65.

Config (PR_0000054554)— The command **copy config <config1 | config2 | config3> config CONFIG** either fails, or creates a CONFIG file with invalid parameters.

Config (PR_0000054730)— For a switch with two configuration files that contain SSH keys, when the inactive config file is deleted by the user, in some cases the SSH keys are erroneously removed from the active config file.

Config (PR_0000057944) — After a software update the TACACS and RADIUS keys are deleted from the configuration file.

Crash (PR_0000047343)— If Spanning Tree Protocol is enabled when 256 VLANs are already configured on the switch, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception at buffers.c:3323 -- in 'mGvrpCtrl', task ID = 0x5dace40
```

Crash (PR_0000056868) — In some cases with DHCP snooping enabled globally and on a VLAN, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception at alloc_free.c:646 -- in 'tDevPollTx', task ID = 0xa9a1300
-> buf already freed by 0x0A96BC00, op=0x00000000
```

DHCP Snooping (PR_0000056774) — When DHCP snooping is enabled, valid PXE boot packets that have yiaddr = 0.0.0.0 are dropped by the switch.

Enhancement (PR_0000046912)— Adds support for LLDP-PoE+. For more information, see “LLDP PoE+ Enhancements” on page 147.

Enhancement (PR_0000054059)— Adds the ability to configure the **console local-terminal** settings without entering config mode. For more information, see “Console Local—Terminal None” on page 150.

File Transfer (PR_0000057021)— A remote client is unable to copy the switch's config file via SCP or SFTP.

File Transfer (PR_0000057616) — In rare situations the switch might not correctly download a config file, reporting `invalid input` errors.

MAC Authentication (PR_0000046430) — The HTTP redirect feature for MAC Authentication clients that fail initial authentication does not work.

SNMP (PR_0000050869)— An SNMP query for hpChassisTemperature always returns a value of 4 (indicating good), even when the output of **show system temperature** indicates the switch is overheated.

Release K.14.66

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.66.

Authentication (PR_0000048471) - In a situation where four RADIUS servers are configured in a Default Server Group and the first server is removed from the configuration, the switch does not attempt to authenticate a user against the fourth configured server.

CDP (PR_0000056202) - When CDP is disabled with the CLI command **no cdp run**, the switch forwards CDP packets it receives.

Crash (PR_0000056925) - When a user has scheduled a reboot time for the switch using the commands **reload at** or **reload after**, the switch might reboot unexpectedly when it reaches the scheduled time, with a message similar to one of the following.

```
NMI event HW:IP=0x00fdeaa0 MSR:0x02029200 LR:0x00fdea8c
cr: 0x40000000 sp:0x03b56910 xer:0x20000000
Task='eDevIdle' Task ID=0xa9a4000
```

```
NMI event HW:IP=0x00fb4eac MSR:0x02029200 LR:0x00fb4e9c
cr: 0x28000800 sp:0x031e6d78 xer:0x20000000
Task='tDevPollRx' Task ID=0xa9a2000
```

Crash (PR_0000057492) - If the UDLD **link-keepalive** timer is turned on and off repeatedly, the switch might reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at svc_timers.c:820 -- in 'mSnmpCtrl', task ID = 0xa9417c0
```

MSTP (PR_0000058462) - Under certain circumstances, the switch might increment the Topology Change Count when it should not. The topology change is incorrectly detected on a link that is blocked at the far end.

Stacking (PR_0000056316) - After refreshing the close-up view in a web browser several times, stack members may time out and may no longer be displayed.

TACACS (PR_0000054391) - When the TACACS server key and switch TACACS key do not match, failover to local authentication does not function properly.

USB (PR_0000055770) - When the user copies a configuration file to USB and there is an existing file with the same name and the existing file is larger than the new file, then remnants of the previous configuration file may appear in the new file.

Release K.14.67

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.67.

Authentication (PR_0000058602) - A client using 802.1X, Web, or MAC authentication might lose access to the network immediately after being authenticated.

Config (PR_0000054554) - The command **copy config <config1 | config2 | config3> config CONFIG** either fails, or creates a CONFIG file with invalid parameters.

Enhancement (PR_0000052266) - Adds the ability to enable an SNMP trap when the switch's startup configuration is changed. For more information, see “Log Message When Startup Config Updated” on page 151.

OSPF (PR_0000058797) - With OSPF and VRRP enabled, a route to a specific host might be lost during a VRRP failover. The switch will display this event log message: `IpAddrMgr: Failed to add FIB entry - route matches existing next-hop router`.

Release K.14.68

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.68.

CLI (PR_0000059255) - Attempts to configure a valid IPv4 syslog server address (command **logging <ip-address>**) might fail with an `inconsistent value` error message.

CPU Utilization (PR_0000059792) - Certain situations with ECMP, a large number of routes (on the order of 3000), or use of the **clear arp** command, may result in high CPU utilization and decreased performance on the switch.

Event Log (PR_0000059300) - Event log message #608 displays `vlan 0` instead of a valid failure type.

Port Communication (PR_0000060305) - The interrupt-driven port-down notification introduced in K.14.66 may, in rare situations, cause a port to block outgoing traffic after a switch reboot.

UDLD (PR_0000058636) - A port that is configured for UDLD may be in a UDLD blocking state for five seconds after the link comes up, which can cause issues with VRRP.

Release K.14.69

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.69.

LLDP (PR_0000058583) - After a switch port loses link, the output of **show power brief <port_number>** wrongly indicates that no PoE power is being delivered.

PIM-DM (PR_0000059788) - In an OSPF ECMP environment where two routers forward the multicast flows, some hosts might receive only half the multicast channels. Workaround: increment the OSFP cost on one of the equal-cost links, to remove the equal-cost issue while retaining network redundancy.

QOS (PR_0000060250) - When software is updated from K.13 to K.14, the QOS device-priority mask-lengths are changed.

Release K.14.70

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.70.

Enhancement (PR_0000055367) - Adds the ability to log ACL "permit" entries. For more information, see “Logging for Routing ACLs” on page 152.

OSPF (PR_0000061138) - This PR_0000061138 improves the original OSPF fix (PR_0000055768, in K.14.64) regarding the Shortest Path First (SPF) counter.

TELNET (PR_0000061481) - When connecting to the switch via TELNET, if a router between the client and the switch has an MTU setting of less than 1500 bytes, the first attempt to TELNET fails.

Release K.14.71

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.71.

Banner MOTD (PR_0000060976) - The switch does not write the login banner to the configuration when the login banner contains 1137 or more characters and the configuration file is downloaded to the switch.

CLI (PR_0000059016) - When the user types **logout** from a console session, the switch closes the session without the `Do you want to log out [y/n]?` and `Do you want to save current configuration [y/n/^C]?` prompts.

CLI (PR_0000060965) - The CLI response to **sho int eth <port_number>** displays only the second half of the first byte of the MAC address. The switch response to **show mac** and other commands that list the MAC address accurately display the proper format of MAC addresses.

CLI (PR_0000061308) - The output of the command **show mac-address <port-list>** lists only MAC addresses in VLAN 1 on the specified ports.

CLI (PR_0000061404) - After configuring an SFP slot with the CLI command **speed-duplex 100-half** and saving the configuration, that setting is erased when the switch reboots.

CPU Utilization (PR_0000061703) - Certain situations with ECMP, a large number of routes (on the order of 3000), or use of the **clear arp** command, may result in high CPU utilization and decreased performance on the switch. This fix improves the original fix (PR_0000059792) in K.14.68.

Rate Limiting (PR_0000045467) - Ingress rate-limiting that is configured via RADIUS or Identity Driven Manager (IDM) is not applied to OSI Layer 2 traffic.

SNMP (PR_0000060189) - The MIB object "dot3PauseOperMode" has incorrect information about the state of flow control on a port.

TELNET (PR_0000061045) - After opening and then closing a Telnet session to another switch, the message `Telnet closed: Connection reset by peer` is displayed instead of `Telnet closed: Connection closed by host`.

Web Authentication (PR_0000050691) - When customized pages for web authentication have been created on a web server, then after rebooting the switch or after making configuration changes to the port that is configured for web-based authentication, an authenticating user is presented with the internal web pages instead of the customized pages.

Release K.14.72

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.72.

CLI (PR_0000053222) - The CLI command **snmp-server trap-source** does not allow the user to configure the Out of Band Management (OOBM) IP address as the trap source.

CLI (PR_0000061523) - The command **clear intrusion-flag** only clears the intrusion flag on the first port.

CLI (PR_0000061904) - When a user displays a named configuration file by issuing the command **show config <filename>**, the switch displays the default configuration after the actual configuration.

Crash (PR_0000002878) - When the switch is configured as a stack member, it will reboot continuously when the following configuration options are applied.

- A default gateway is configured on the stack member
- An IP address is configured on VLAN 1 of the stack member
- The stack member adds a new SNMP community name (in addition to "public"), with manager MIB view
- The stack commander adds the same new community name, with manager MIB view
- The stack commander adds a trap receiver for community name "public"

The switch will log a crash message similar to the following.

```
TLB Miss:  Virtual Addr=0x00000009 IP=0x800bd660 Task='mSnmpEvt'
Task ID=0x81e040d0 fp:0x00000000 sp:0x81e03f18 ra:0x800bd5d0 sr:0x1000fc01
```

Crash (PR_0000061028) - After a user reconfigures the console settings and reboots the switch, opening a second session may result in a situation where both console sessions are unresponsive. When left in this state, the switch may eventually reboot unexpectedly with a message similar to the following.

```
Software exception at watchdog.c:446 -- in 'tSvcWorkQ', task ID = 0x1cea5240.
```

Mirroring (PR_0000062574) - When a user has configured remote mirroring on a K.13.xx release and is monitoring a VLAN, then booting to a K.14.xx release causes the remote mirror configuration to be removed from the configuration.

SNMP (PR_0000060257) - The port type for 100-BX and 1000-BX transceivers is incorrectly identified when requested via SNMP.

Syslog (PR_0000012167) - Syslog messages longer than 119 characters get truncated.

Web Management (PR_0000060813) - Using the Web interface, the close-up view of stack members might not display if the commander is configured for SSL-only access.

Release K.14.73

Status: Never released.
The following problems were resolved in software version K.14.73.

CLI (PR_0000057810) - Some switch responses are displayed on a single line, when they should be displayed on two separate lines.

Counters (PR_0000062966) - The Drops Tx counter is not reset when a port goes offline, which can cause erroneous FFI (Find, Fix, Inform) `High collision or drop rate` messages after the port comes back online.

Port Communication (PR_0000061884) - A PoE+ switch port configured with **speed-duplex auto-10-100** and connected to an Intel NIC 82566 with Wake on LAN enabled might stop responding after one or two hours. Workaround: configure the port with the **speed-duplex auto** setting.

SNMP (PR_0000061912) - The MIB object hpicfReloadControl (OID 1.3.6.1.4.1.11.2.14.11.1.4.20.2.2.1.1) was implemented to add the ability to reload individual modules in a modular switch. When a user runs an **snmpwalk** against this object on a non-modular switch that does not support this feature, the switch incorrectly returns responses.

Release K.14.74

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.74.

Authentication (PR_0000058253) - The switch's event log reports `auth: Invalid user name/password on SSH session`, even though the client is already authenticated.

Crash (PR_0000055261) - In some situations the switch might reboot unexpectedly with a message similar to the following.

```
SubSystem 0 went down: 06/22/10 09:24:00
NMI event SW:IP=0x00e953d8 MSR:0x02029200 LR:0x00eb25c8
cr: 0x24000400 sp:0x02e30aa8 xer:0x20000000
Task='InetServer' Task ID=0xaad5000
```

Crash (PR_0000061416) - On a switch that has DHCP-snooping enabled, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception at alloc_free.c:575 -- in 'tDevPollTx', task ID = 0xa9a6d80
-> buf already freed by 0x0A91A180, op=0x00000000
```

Release K.14.75

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.75.

CLI (PR_0000060966) - Changing the terminal width to values larger than 100 might cause CLI messages to be truncated.

Enhancement (PR_0000063482) - The **copy command-file** feature now works for configuration commands other than ACLs.

Module Crash (PR_0000064847) - A switch module might reboot unexpectedly with a message similar to the following.

```
Software exception in ISR at buffers.c:3222
-> ASSERT0:  failed
```

PIM (PR_0000064763) - PIM register packets are dropped by the switch if the checksum is calculated over the entire packet.

Stacking (PR_0000062828) - After an Operator password is configured on the stack commander, that switch stops responding to console commands.

Release K.14.76

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.76.

802.1X (PR_0000005372) - Some combinations of source and destination MAC addresses may cause 802.1X to stop functioning on a port; only a reboot will recover functionality.

ACLs (PR_0000059674) - After updating switch software from K.13.58 or later (with a K.13 config file) to K.14 software, ACL rate-limit commands that are applied to multiple interfaces are duplicated for each interface in the config file. That is, a uniquely-numbered but identical policy is created for each interface, instead of applying a single policy to each interface. The policies function properly, but the config file is more difficult to interpret.

ACLs (PR_0000061483) - The Access Control Entry (ACE) **permit tcp any <destination_IP> established** does not function properly.

CLI (PR_0000015073) - When a trunk is monitored by a mirror port, a user is allowed to remove the trunk from the configuration even if monitoring has not been disabled first.

CLI (PR_0000056366) - The switch does not list the command options when pressing the **<Tab>** key. This only affects commands that contain an ACL name between quotation marks.

CLI (PR_0000061969) - The switch responds with `translator failed` messages when the user enters **copy config** and **show tech** commands. This is seen with very large configuration files.

LLDP-MED (PR_0000038954) - After rebooting, a switch with more than 25 phones connected may not place all the phones in the correct VLAN.

Routing (PR_0000062927) - When routing large files, packet loss may be experienced if hosts and IP routes are being added to and/or removed from the routing tables during the file transfers.

SSH (PR_0000063910) - After enabling SSH and removing TELNET service, the switch does not respond to SSH management via Opsware NCM.

Transceivers (PR_0000062554) - When the switch is rebooted with a BX transceiver inserted, after boot the switch does not display the transceiver's information in the output of `show tech transceiver`. This only affects the BX transceiver that has the highest port number.

Release K.14.77

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.77.

Authentication (PR_0000058441) - User authentication fails if the user's Radius configuration includes a non-HP VSA before any HP VSAs. Workaround: Configure the user in Radius with at least one HP VSA before any non-HP VSAs.

CLI (PR_0000043470) - The switch has a prerequisite to configure an IPv4 loopback address before configuring any IPv6 address on the switch. When the user attempts to configure an IPv6 address before configuring an IPv4 loopback address, the error message is confusing. This fix provides an improved error message.

Event Log (PR_0000064762) - Event log message #609 displays `vid 0` instead of a valid VLAN ID.

Instrumentation Monitor (PR_0000053498) - Some of the instrumentation counters are always set to '`0`'.

IPv6 (PR_0000063303) - When a VLAN is configured as a Management VLAN and the switch is rebooted, IPv6 features such as DHCPv6, IPv6 routing and Neighbor Discovery stop working.

LLDP-MED (PR_0000062113) - The switch uses the default QoS priority of 6 for the voice VLAN, no matter what priority is configured.

MAC Authentication (PR_0000063756) - The switch does not respond to or learn from incoming packets with the same source and destination MAC addresses, which causes MAC authentication to fail.

OSPF (PR_0000008723) - The OSPF area LSDB checksum is not the same for routers that reside in the same area and have the same LSAs.

Routing (PR_0000043311) - IP addresses configured on interface loopback 0 are not used after a reboot of the switch.

Release K.14.78

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.78.

CLI (PR_0000062213) - When a single MAC address exists in multiple VLANs on a port, the output of the command **show mac-address <port>** lists that MAC address in only one VLAN on the specified port.

CLI (PR_0000064363) - When a user issues the command **show interfaces all** on a chassis that has no modules inserted, the system generates the error message `Cannot use a member of a trunk: all`.

Crash (PR_0000064620) - When a trunk type is changed from **trunk** to **LACP**, if the trunk is a higher-numbered trunk (e.g. trk11) and has an access group applied, the switch might reboot unexpectedly with a message similar to the following.

```
Execute Access Error - Restricted Memory
Exception number: 0xdead0300
HW Addr=0x70000000 IP=0x70000000 Task='mSnmpCtrl' Task ID=0x1a47e9c0
fp: 0x72756769 sp:0x
```

Crash (PR_0000067153) - With a local password configured, after using the Web interface to access the Configuration Report the switch might reboot unexpectedly with a message similar to the following.

```
Write Error - Restricted Memory Exception number: 0xdead0200
  HW Addr=0x20706900 IP=0x10cb0330 Task='mSess1' Task ID=0x1a470480 fp:
  0x126a0964 sp:0x126a0950 cps
```

Crash Messaging (PR_0000015799) - Important data may be truncated from the crash message.

SNMP/IPv6 (PR_0000039353) - An SNMP walk of the ipAddressType at the switch CLI (**walkmib 1.3.6.1.2.1.4.34.1.4**) erroneously shows all IPv6 address types as '`anycast`'.

Transceivers (PR_0000067460) - The transceiver in the highest numbered port will not establish link after a reboot of the switch. Workaround: remove, then re-insert the transceiver.

Web Management (PR_0000061436) - When the URL **http://<ip-address>/configuration/device_viewf.html** is requested from the switch, the switch returns the error '`Bad Request`'. This URL is used to display the front panel of the switch and is used for the Live View in PCM.

Release K.14.79

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.79.

CLI (PR_0000064511) - The switch might become unresponsive to management after issuing the CLI command **show connection-rate-filter all**.

CLI (PR_0000067688) - The output of the **show system** command might display an incorrect value for Free Memory.

Crash (PR_0000064556) - When a user removes the source-ip-vlan on a PIM SM router that is actively routing multicast traffic and then adds the source-ip-vlan again, router might reboot unexpectedly with a message similar to the following.

```
Software exception at alloc_free.c:575 -- in 'mPimsmCtrl', task ID = 0xa90c280
-> buf already freed by 0x0A90C280, op=0x00440002
```

Crash (PR_0000066570) - After a large number of startup configuration changes, the switch might reboot unexpectedly with a message similar to the following.

```
Unable to allocate message buffer
Software exception in ISR at btmDmaApi.c:370
```

Event Log (PR_0000060511) - When the switch experiences a brief power outage, the event log might give erroneous indications regarding the cause and the results. Specifically, the switch might report that a) the switch rebooted due to the reset button being pressed, and b) the switch booted from secondary flash because primary flash is corrupt. Both these indications are false. The output of **show version** confirms that the switch booted from primary flash and is running the software from primary flash.

Instrumentation Monitor (PR_0000065498) - The system delay value might be incorrectly displayed as a negative number.

SSH (PR_0000060114) - With a large terminal length setting, if the switch output is on the order of 100 lines or more, the switch will appear to "hang" until the user presses **<Enter>** on the console. Workarounds: Use the **no page** command, or use the default terminal length setting (24 lines).

SSL (PR_0000064686) - After copying the CA certificate to the switch this error message is received: `Error setting CA Signed Request Configuration - No certificate is installed`.

Release K.14.80

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.80.

Authentication (PR_0000068384) - When a PC is plugged into a VOIP phone and authenticated on that switch port, if the PC is moved to another VOIP phone without first logging out of Windows, authentication fails.

DHCP Snooping (PR_0000067680) - The DHCP snooping database is not uploaded to or downloaded from the external TFTP server if **no tftp server** is configured on the switch.

Transceivers (PR_0000068539) - When the switch is rebooted with a BX transceiver inserted, after boot the switch does not display the transceiver's information in the output of **show tech transceiver**. This only affects the BX transceiver that has the highest port number. This improves the original fix (PR_0000062554) in K.14.76.

Release K.14.81

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.81.

ARP (PR_0000068610) - After 497 days of system uptime, ARP cache entries might no longer age out.

Distributed Trunking (PR_0000067601) - When a Distributed Trunk port goes offline and comes back online, the Distributed Trunk port does not forward traffic for 30 seconds.

Event Log (PR_0000061889) - Event log entries for Dynamic ARP Protection are throttled, even when they are triggered by different clients.

Power (PR_0000066248) - When the switch is exposed to AC power fluctuations that cause voltage drops, some modules might lose power and not recover.

Routing (PR_0000040779) - When a RIP router needs to send more than 25 routes in an update, it will send the first 25 routes in the first update and will start the second update with the 27th route. The router skips the 26th route.

Trunking (PR_0000067623) - After a switch reboot, traffic might not be forwarded across a static port-based trunk. This might happen if an LACP Distributed Trunk is also configured on the switch and the Distributed Trunk has higher-numbered ports than the static port-based trunk.

Release K.14.82

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.82.

CLI (PR_0000050800) - The output of the CLI command **show tech instrumentation** displays incorrect values for `port toggles`.

Instrumentation Monitor (PR_0000068741) - The system displays an incorrect value for the IP Addr Count#. If the Instrumentation Monitor is configured to track that counter value, the system may generate incorrect event log messages warning the user that the threshold value has been exceeded.

SNMP (PR_0000064215) - An SNMP query for the authorized VLAN ID or the unauthorized VLAN ID does not receive a correct value.

TACACS (PR_0000067897) - When a configuration file is downloaded to the switch and the file contains a separate configuration entry for the TACACS key, after the switch is rebooted, authentication via TACACS may fail with this message: `00983 tacacs: malformed packet received from <IP address> server`.

Release K.14.83

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.14.83.

Authentication (PR_0000017310) - When a PC is attached to the PC port of a VoIP phone and the PC authenticates first (before the phone), the switch does not use the RADIUS-assigned tagged VLAN for the phone, so the phone does not authenticate.

Crash (PR_0000066287) - On K.15.xx a user can configure an IPv6 address on a loopback interface. When a switch is booted to a K.14.xx version that does not support this configuration, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception at dhcpv6c_ctrl.c:850 -- in 'mDhcpv6CCtl', task ID = 0xa964680
-> Invalid Vid: 4096. Valid vid range is from 1 to 4094
```

Crash (PR_0000067140) - When SSH sessions are established with the switch or are disconnected, sometimes the switch might reboot unexpectedly with a message similar to the following.

```
Access Violation - Restricted Memory
Exception number: 0xdead0000
HW Addr=0x2c030000 IP=0x00002670 Task='tSshcnn' Task ID=0xa90e780
fp: 0x00000000 sp:0x04ac032
```

FFI (PR_0000070023) - The switch does not create an entry in the event log when the threshold for certain FFI (Find, Fix, Inform) events is met.

File Transfer (PR_0000063877) - Using the CLI command **copy flash flash < primary | secondary >** from an SSH session might cause the SSH session to disconnect. However, the file transfer completes successfully.

Transceivers (PR_0000068009) - When a 1000BASE-T transceiver (J8177B/C) is inserted into a slot with configured speed-duplex settings that are not valid for that transceiver, the switch does not set the speed-duplex settings to their default values, which might cause an interface module on a chassis to reboot unexpectedly.

Release K.14.84

Status: Released and fully supported and posted on the Web.
The following problems were resolved in software version K.14.84.

IPv6 (PR_0000068744) - The output of **show ipv6 routers** lists router preference as medium. This field was removed.

PIM (PR_0000070281) - PIM register packets are dropped by the switch if the checksum is calculated over the entire packet and the packet size is an odd number of bytes.

SSL (PR_0000070330) - After copying the CA certificate to the switch this error message is received: `Error setting CA Signed Request Configuration - No certificate is installed`.

Technology for better business outcomes

To learn more, visit www.hp.com/networking/

June 2011

Manual Part Number
5992-5498